

**CCTV  
CODE OF PRACTICE**

**FOR**

**West Midlands Combined Authority  
(WMCA)  
CONTROL CENTRE**

**CODE OF PRACTICE FOR CCTV SCHEME  
(BS 7958)**

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

Page: 2 of 44

Authority:

M.Sayers

Date: February 2021

### CONTENTS

<b>1..0</b>	<b>INTRODUCTION AND DEFINITIONS</b>	<b>4</b>
<b>1.2</b>	OWNERSHIP	<b>4</b>
<b>1.3</b>	CCTV MISSION STATEMENT	<b>4</b>
<b>1.4</b>	CODES OF PRACTICE MISSION STATEMENT	<b>4</b>
<b>1.5</b>	DEFINITIONS	<b>4</b>
<b>1.6</b>	SYSTEM DESCRIPTION	<b>6</b>
<b>2.0</b>	<b>CHANGES TO THE CODE OF PRACTICE</b>	<b>8</b>
<b>2.1</b>	CONSULTATION	<b>8</b>
<b>2.2</b>	SUPPLEMENTARY DOCUMENTATION	<b>8</b>
<b>3.0</b>	<b>OBJECTIVES OF THE CCTV SCHEME AND CODE OF PRACTICE</b>	<b>9</b>
<b>3.1</b>	PURPOSE OF AND COMPLIANCE WITH CODE OF PRACTICE	<b>9</b>
<b>3.2</b>	OBJECTIVES OF THE SCHEME	<b>9</b>
<b>4.0</b>	<b>FUNDAMENTAL PRINCIPLES AND POLICIES</b>	<b>11</b>
<b>4.1</b>	RIGHTS OF PRIVACY	<b>11</b>
<b>4.2</b>	PRINCIPLES OF MANAGEMENT OF THE SCHEME	<b>11</b>
<b>4.3</b>	POLICY OF THE SCHEME AND SIGNAGE	<b>12</b>
<b>4.4</b>	POINT OF CONTACT	<b>12</b>
<b>4.5</b>	SAFETY AND INTEGRITY OF THE SCHEME	<b>12</b>
<b>4.6</b>	RELEASE OF INFORMATION TO PUBLIC	<b>12</b>
<b>4.7</b>	RELEASE OF INFORMATION TO STATUTORY BODIES	<b>13</b>
<b>4.8</b>	ANNUAL POLICY REVIEW	<b>13</b>
<b>5.0</b>	<b>DATA PROTECTION AND LEGISLATION</b>	<b>14</b>
<b>5.1</b>	DATA PROTECTION REGISTRATION	<b>14</b>
<b>5.2</b>	HUMAN RIGHTS ACT 1998	<b>15</b>
<b>5.3</b>	CRIMINAL PROCEDURES AND INVESTIGATIONS ACT 1996	<b>15</b>
<b>5.4</b>	FREEDOM OF INFORMATION ACT 2000	<b>15</b>
<b>5.5</b>	REGULATION OF INVESTIGATORY POWERS ACT 2016	<b>16</b>
<b>5.6</b>	SURVEILLANCE CAMERA CODES	<b>17</b>
<b>5.7</b>	CRIME AND COURTS ACT 2013	<b>18</b>
<b>6.0</b>	<b>ACCOUNTABILITY</b>	<b>19</b>
<b>6.1</b>	SUPPORT OF PRINCIPLES	<b>19</b>
<b>6.2</b>	RESPONSIBILITIES	<b>19</b>
<b>6.3</b>	ACCOUNTABILITY	<b>21</b>
<b>6.4</b>	ANNUAL ASSESSMENTS	<b>21</b>
<b>6.5</b>	AUDITS	<b>22</b>
<b>6.6</b>	COMPLAINTS	<b>22</b>
<b>6.7</b>	PERSONNEL	<b>23</b>
<b>7.0</b>	<b>CONTROL ROOM MANAGEMENT AND OPERATION</b>	<b>24</b>
<b>7.1</b>	GENERAL	<b>24</b>
<b>7.2</b>	RESPONSE TO INCIDENTS	<b>24</b>
<b>7.3</b>	MAKING RESPONSE AND TIME SCALES	<b>24</b>
<b>7.4</b>	OBSERVATION AND RECORDING INCIDENTS	<b>25</b>
<b>7.5</b>	SUCCESSFUL RESPONSE	<b>25</b>
<b>7.6</b>	OPERATION OF THE SYSTEM BY POLICE	<b>25</b>

**CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES**

<b>Page: 3 of 44</b>	<b>Authority: M.Sayers</b>
<b>Date: February 2021</b>	

<b>8.0</b>	<b>PRIVACY AND DISCLOSURE ISSUES</b>	<b>26</b>
<b>8.1</b>	PRIVACY	<b>26</b>
<b>8.2</b>	DISCLOSURE POLICY	<b>26</b>
<b>8.3</b>	ACCESS TO RECORDED IMAGES	<b>27</b>
<b>8.4</b>	VIEWING OF RECORDED IMAGES	<b>27</b>
<b>8.5</b>	OPERATORS AWARENESS	<b>27</b>
<b>8.6</b>	REMOVAL OF MEDIUM FOR VIEWING	<b>27</b>
<b>8.7</b>	ACCESS TO DATA BY THIRD PARTIES	<b>27</b>
<b>8.8</b>	DISCLOSURE IN THE PUBLIC INTEREST	<b>28</b>
<b>8.9</b>	DATA SUBJECT ACCESS	<b>28</b>
<b>8.10</b>	PROVISION OF DATA TO INDIVIDUALS	<b>29</b>
<b>8.11</b>	OTHER RIGHTS	<b>29</b>
<b>8.12</b>	MEDIA DISCLOSURE	<b>30</b>

<b>9.0</b>	<b>RECORDED MATERIAL MANAGEMENT</b>	<b>31</b>
<b>9.1</b>	GENERAL	<b>31</b>
<b>9.2</b>	QUALITY AND MAINTENANCE	<b>31</b>
<b>9.3</b>	DIGITAL RECORDING	<b>31</b>
<b>9.4</b>	MAKING RECORDINGS	<b>32</b>
<b>9.5</b>	PRINTS	<b>32</b>

<b>10.0</b>	<b>DOCUMENTATION</b>	<b>33</b>
<b>10.1</b>	GENERAL	<b>33</b>
<b>10.2</b>	LOGS	<b>33</b>
<b>10.3</b>	ADMINISTRATIVE DOCUMENTS	<b>33</b>

<b>Appendix A</b>	<b>SUBJECT ACCESS FORM</b>	<b>34</b>
<b>Appendix B</b>	<b>SCHEME LEAFLET</b>	<b>39</b>
<b>Appendix C</b>	<b>CERTIFICATE OF AGREEMENT</b>	<b>43</b>

Page: 4 of 44	Authority: M.Sayers
Date: February 2021	

## 1.0 INTRODUCTIONS & DEFINITIONS

### Introduction

**1.1** This Code of Practice shall apply to the closed circuit television surveillance scheme known as the WMCA CCTV scheme. The scheme initially comprises of cameras located in specific external and internal locations of the WMCA area with control, monitoring and recording facilities at a dedicated location. A problem orientated process was utilised to assess the appropriateness of CCTV in the WMCA locations. The cameras have therefore been sited to capture images of identifiable individuals or information relating to individuals which are relevant to the purposes for which the scheme has been established.

### 1.2 Ownership

The scheme is owned by WMCA who is responsible for the management and security of the system. WMCA will ensure the protection of individuals and the public by complying with the Codes of Practice. The Single Point of Contact for WMCA is the Data Protection Information Sharing officer.

### 1.3 Closed Circuit Television Mission Statement

To promote public confidence by developing a safe and secure environment for the benefit of those employed, visiting or using the facilities provided by WMCA. WMCA is committed to the recommendations contained in the Surveillance Camera Commissioner's Code of Practice and the Information Commissioners CCTV Code of Practice which can be found on the following websites: [www.gov.uk/government/organisations/surveillance-camera-commissioner](http://www.gov.uk/government/organisations/surveillance-camera-commissioner) and [www.ico.gov.uk](http://www.ico.gov.uk).

### 1.4 Codes of Practice Mission Statement

To inspire public confidence by ensuring that all public area Closed Circuit Television (CCTV) systems which are linked to the CCTV Control and Monitoring Room are operated in a manner that will secure their consistent effectiveness and preserve the civil liberty of law abiding citizens at all times.

### 1.5 Definitions

**1.5.1 The CCTV Monitoring Centre** secure location for a CCTV scheme where images are collected, used, disclosed retained and disposed of. It is also the location where calls may be received from 'Help Points' and from where warning can be made via public address systems, associated with the cameras.

**1.5.2 CCTV scheme** shall mean the totality of the arrangements for closed circuit television in the locality and is not limited to the technological system, staff and operational procedures.

**1.5.3 CCTV system** means the surveillance items comprising cameras and associated equipment for monitoring, recording, transmission and controlling purposes, for use in a defined zone.

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

<b>Page:</b> 5 of 44	<b>Authority:</b> M.Sayers
<b>Date:</b> February 2021	

- 1.5.4 The **public address system** means the equipment connected to CCTV cameras and associated equipment installed at the WMCA Control room, which allows the CCTV operators to address the public
- 1.5.5 **Help Points** are button operated units located at WMCA facilities, which are linked to the control room and allow the public to communicate directly with an operator in the Control Room in the event of an emergency
- 1.5.6 **Contractor**, party contracted by the owner to undertake agreed services
- 1.5.7 **Controlled environment** anywhere that data which might be offered as evidence is received, stored, reviewed or analyzed including at the CCTV Monitoring Centre.
- 1.5.8 **Data** shall mean all information, including that about a person in the form of pictures, and any other associated linked or processed information.
- 1.5.9 **Personal Data** means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. Identifiers include images, name, identification number, location data, or online identifier.
- 1.5.10 **Special Category data** is personal data which is deemed to be sensitive. The most significant of these, for the purposes of this code are information about:-
- The commission or alleged commission of any offences
  - Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.
- 1.5.11 **An incident** is an activity that warrants a response.
- 1.5.12 **The owner** is, West Midlands Passenger Transport Executive (WMCA) the organisation with overall responsibility for the formulation and implementation of policies, purposes and control of the scheme.
- 1.5.13 **Privacy impact assessment** of the impact a CCTV system has on an individual's right to privacy.
- 1.5.14 **The systems manager** has the responsibility for the implementation of the policies, purposes and methods of control of a CCTV scheme, as defined by the owner of the scheme. The systems manager means the Safer Travel Manager.
- 1.5.15 **Data controller** means a 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, or are about to be processed.
- 1.5.16 **Operators** are employed by the Contractor and are specifically designated to carry out the physical operation and control of the WMCA CCTV system and the data generated. All operators are screened, trained and licensed to the standards required in the Private Security Industry Act 2001.

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

<b>Page:</b> 6 of 44	<b>Authority:</b> M.Sayers
<b>Date:</b> February 2021	

1.5.17 **Recording material** means any medium that has the capacity to store data and from which data can later be recalled irrespective of time.

1.5.18 **A hard copy print** is a paper copy of a live image or images, which already exist on recorded material.

### 1.6 System description

1.6.1 The CCTV systems referred to in this document have been installed into the WMCA / Solihull / Walsall / East Staffordshire / Tamworth areas. Whilst the schemes are owned by WMCA / Solihull / Walsall / Tamworth / East Staffordshire Metropolitan Borough Council respectively, its implementation and/or expansion is supported by the following bodies (the partners):

- West Midlands Police
- British Transport Police
- Train Operating Companies

The WMCA / Solihull / Walsall / Tamworth / East Staffordshire Metropolitan Borough Council CCTV's system is managed operated and monitored by WMCA under agreement.

The owners, operator and all partners will work in accordance with the Codes. The partners will have no involvement in the operating of the system with the exception of the Police as outlined later in this document.

1.6.2 This Code of Practice shall apply to the CCTV systems, including re-deployable systems owned and operated by WMCA /Solihull / Walsall / Tamworth / East Staffordshire Metropolitan Borough Council. The CCTV systems referred to in this document have been introduced to rail and bus station interchanges throughout the West Midlands in respect of WMCA and into the WMCA / Solihull / Walsall / Tamworth / East Staffordshire area.

1.6.3 The system consists of static and fully functional (pan, tilt and zoom) cameras at the locations mentioned in the previous paragraph and include a transmission system that sends pictures to the WMCA control, monitoring and recording facility.

1.6.4 The WMCA public address system consists of speakers attached to fully functional cameras at specific sites, which are linked to the control room from where operators can address the public while viewing the immediate locality.

1.6.5 A WMCA help point consists of a unit located at the station or car park in a position of easy access, with a button to press for use in emergencies. Operation of the help point allows two-way communication between caller and the control room staff. In the control room, messages are automatically recorded together with the pictures from the camera viewing the help point.

1.6.6 Images from all cameras are recorded simultaneously throughout 24 hour period 365 days each year.

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

<b>Page: 7 of 44</b>	<b>Authority: M.Sayers</b>
<b>Date: February 2021</b>	

- 1.6.7 There is also a dedicated CCTV transmission link to Police control room operating within the areas of CCTV coverage where live pictures and events can be monitored.
- 1.6.8 High quality cameras both fully functional with pan, tilt and zoom and static are in use.
- 1.6.9 The physical and intellectual rights in relation to any and all material recorded within the WMCA Control and Monitoring facility shall at all times remain in the ownership of WMCA / Solihull / Walsall / Tamworth / East Staffordshire Council respectively.

## 2.0 CHANGES TO THE CODE OF PRACTICE

**2.1** Any major changes to this Code of Practice will take place only after consultation with the relevant management group and upon agreement of all organisations with a participatory role in the operation of the system.

**2.1.1** Major changes to this code are defined as changes which affect its fundamental principles and shall be deemed to include:

- additions and omissions of cameras to the system
- matters which have privacy implications
- additions to permitted uses criteria e.g. purposes of the scheme
- changes in the right of access to personal data, except statutory requirements
- significant legal implications.

**2.1.2** Minor changes to this Code of Practice are defined as operational and procedural matters which do not affect the fundamental principles and purposes; these include:

- additions and omissions of contractors
- additional clarifications, explanations and corrections to the existing code
- additions to the code of practice in order to conform to the requirements of any statutory Acts and changes in criminal legislation

A minor change may be agreed between the manager and the owner of the system.

The Code of Practice will be subject to annual review which will include compliance with the relevant legislation and Standards.

## **2.2 Supplementary Documentation**

- The Code of Practice will be supplemented by the following documents:
- CCTV Operations Procedural Manual
- Operators Equipment Manual

Each document contains instructions and guidance to ensure that the objectives and principles set out in this Code of Practice are achieved. These documents will be restricted to the partners and staff members only.

### 3.0 PURPOSE OF THE CODE OF PRACTICE & CCTV SCHEME

#### 3.1 Purpose of and Compliance with the Code of Practice

- 3.1.1 This Code of Practice is to detail the management, administration and operation of the CCTV system in the WMCA / Solihull / Walsall / Tamworth / East Staffordshire areas and the associated Control and Monitoring Facility.
- 3.1.2 The Code of Practice has a dual purpose, in that it will assist owners, management and operators to understand their legal and moral obligations whilst reassuring the public about the safeguards contained within it.
- 3.1.3 The owners, CCTV Operators and users of the CCTV systems and associated safety and security equipment connected to the Control, Monitoring and Recording facility shall be required to give a formal undertaking that they will comply with this Code of Practice and act in good faith with regard to the basic principles contained within it.
- 3.1.4 The owners, CCTV Operators, users and any visitors to the Control, monitoring and recording facility will be required to sign a formal confidentiality declaration that they will treat any viewed and/or written material as being strictly confidential and that they undertake not to divulge it to any other person.

#### 3.2 Purpose and objectives of the scheme

- 3.2.1 The following purposes have been established for the WMCA CCTV and associated systems:

**Purpose Description:**

Crime Prevention and detection and the apprehension and prosecution of offenders

**Objectives:**

The following are the objectives for which The West Midlands Combined Authority CCTV system was established:

- a) assist in the prevention and detection of offences
- b) reduce both the real and perceived level of crime
- c) reduce the fear of crime
- d) improve confidence in the rule of law
- e) assist in the apprehension and prosecution of offenders.
- f) gather evidence by a fair and accountable method
- g) create a safer community, improving the quality of life for all by:
  - reducing car crime
  - monitoring public disorder
  - monitoring the movement of people in emergency situations, e.g evacuation
  - providing assistance in civil claims
  - providing assistance with issues relating to public safety and health

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

Page: 10 of 44

Authority:

M.Sayers

Date: February 2021

### Data Controllers further description of purposes include:

- Initiatives under the Crime and Disorder Act.
- Executive premises where the object is the prevention and detection of crime  
Preparation and serving of anti social behaviour orders.
- Community safety programmes.
- Operation of CCTV systems in shopping centres, includes use of closed-circuit television for the monitoring and collection of sound and/or visual images for the purpose of maintaining the security of premises, for preventing crime and investigating crime.
- Safety management
- Including Bus stations, Rail stations, Tram network, Park and ride sites, Bus shelters and for the purpose of monitoring operational activities to include passenger flows, bus movements and problem behaviour.

## 4.0 FUNDAMENTAL PRINCIPLES

### 4.1 Rights of Privacy

4.1.1. WMCA and partners support the individual's right to privacy and will insist that all agencies involved in the provision and use of Public surveillance CCTV systems connected to the control, monitoring and recording facility accept this fundamental principle as being paramount.

### 4.2 Principles of management of the scheme

4.2.1 Prior to the installation of cameras an 'Impact Assessment' to determine whether CCTV is justified and how it will be operated will be undertaken in compliance with the Information Commissioner's CCTV Code of Practice and the Surveillance Camera Commissioner's Code of Practice.

4.2.2 The cameras have been sited to capture images that are relevant to the specified purposes for which the scheme has been established.

4.2.3 Cameras will be sited to ensure that they can produce images of the right quality, taking into account technical and environmental issues

4.2.4 To accomplish the above an 'Operational Requirement' will be completed at the time of the 'Impact Assessment' for each proposed camera to dictate the quality of images required. This is a recommendation of the information Commissioner.

4.2.5 The WMCA Help Points are to be used in conjunction with the cameras. The audio communications incorporated in the help points are initiated by those requiring assistance and cannot be used to record conversations between members of the public.

4.2.6 If wireless transmission systems are used to control CCTV equipment, sufficient safeguards are in place to protect them from being intercepted. (at present, no such wireless transmission system exists)

4.2.7 At specific locations WMCA public address systems are used in conjunction with the cameras to issue warnings to deter person(s) engaging in criminal activity or ant-social behaviour or to alert the public to a situation of imminent danger and for no other purpose.

4.2.8 The scheme will be operated fairly, within the applicable law and only for the purposes for which it is established or which are subsequently agreed in accordance with the Code of Practice.

4.2.9 Operators are aware of the purpose(s) for which the scheme has been established and that the CCTV equipment is only used to achieve the identified purposes.

4.2.10 The scheme will be operated with due regard for the privacy of the individual.

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

<b>Page:</b> 12 of 44	<b>Authority:</b> M.Sayers
<b>Date:</b> February 2021	

- 4.2.11 Before cameras are placed in residential areas the residents in that area will be consulted concerning the proposed system. The results of the consultation will be taken into account.
- 4.2.12 The public interest in the operation of the scheme will be recognised by ensuring the security and integrity of operational procedures.
- 4.2.13 The system will only be operated by trained and authorised personnel.

### **4.3 Policy of the Scheme and Signage**

The scheme aims to provide surveillance of the public areas within the WMCA / Solihull / Walsall / Tamworth / East Staffordshire areas in order to fulfill the stated purposes of the scheme. The area protected by CCTV will be indicated by the presence of signs. The signs will be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment. The signs will state the organisation responsible for the scheme, the purposes of the scheme and a contact telephone number. Data will not be held for longer than necessary and disposal of information will be regulated.

### **4.4 Point of contact**

Should the public wish to make contact with the owners of the scheme they may write to:

Customer Relations  
WMCA  
16 Summer Lane  
Birmingham  
B19 3SD

The contact point will be available to members of the public during office hours. Enquirers will be provided with the relevant documentation.

### **4.5 Safety and Integrity of the Scheme**

The safety and integrity of the CCTV scheme has been considered and policies have developed which include, physical security, IT security and resilience and the vetting and training of staff.

### **4.6 Release of information to the public**

Information will be released to third parties, itemised in Section 8 who can show legitimate reasons for access. They will be required to request any information with reasons in writing and identify themselves.

Information will only be released if the data captures the individual's activities and the reasons are deemed acceptable, the request and release of information complies with current legislation and on condition that the information is not used for any other purpose than that specified.

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

**Page: 13 of 44**

**Authority:**

**M.Sayers**

**Date: February 2021**

Individuals may request to view information concerning themselves held on record in accordance with the Data Protection Act 2018. The procedure is outlined in Section 8.9 of this Code of Practice.

### **4.7 Release of information to statutory prosecuting bodies**

The policy is to assist statutory prosecuting bodies such as the Police, and statutory authorities with powers to prosecute and facilitate the legitimate use of the information derived from the scheme. Statutory bodies may have access to information permitted for disclosure on application to the owner of the scheme or the manager, provided the reasons and statement of purpose, accord with the objectives of the scheme and conditions outlined in section 8.0. The information will be treated as evidential exhibits.

### **4.8 Annual policy review**

There will be an annual policy review covering the following aspects:

- whether the purpose and objectives statements remain valid
- change in extent of the scheme
- contracts with suppliers
- a review of the data protection or legal requirements
- maintenance schedule and performance test of the system
- scheme evaluation findings
- complaints procedure and evaluation

## 5.0 DATA PROTECTION ACT AND OTHER LEGISLATION

### 5.1

The WMCA scheme is registered with the Data Protection Commissioner, Registration Number: Z5897556. The scheme will be managed in accordance with the principles of the Data Protection Act 2018 and the articles of the General Data Protection Regulation (GDPR). The Act encompasses six Data Protection Principles a summary of which follows:

#### **First Data Protection Principle**

The processing of personal data for any of the law enforcement purposes must be lawful and fair.

The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either:

- a) the data subject has given consent to the processing for that purpose, or
- b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority

The above conditions are covered in the purposes for which the scheme was installed.

The definition of Personal Data and Special Category Personal Data can be found in Section one of this Code.

#### **Second Data Protection Principle**

“Personal Data must not be processed in a manner that is incompatible with the purpose for which it was collected”.

#### **Third Data Protection Principle**

“Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed”.

#### **The Fourth Data Protection Principle**

“Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date.”

#### **The Fifth Protection Principle**

“Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed”.

Page: 15 of 44	Authority: M.Sayers
Date: February 2021	

## The Sixth Data Protection Principle

“Personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)”.

### 5.2 Human Rights Act 1998

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

- 1 Everyone has the right to respect for his private and family life, his home and his correspondence.
- 2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Therefore, to comply with Article 8 (1), and Article 8 (2) the WMCA CCTV Service will always consider the following:

- Proportionality - Article 4.2.1, 4.2.2, 4.2.3 and 4.2.6 of the code of practice
- Legality - Article 4.2.7 and 4.2.8 of the code of practice
- Accountability - Article 4.2.10 and 4.2.11 of the code of practice
- Necessity/Compulsion - Article 4.2.3 of the code of practice

Any infringement by a public authority of another’s rights must be justified. If this is not the case then it will not be appropriate to use CCTV.

### 5.3 Criminal Procedures and Investigations Act 1996

The Criminal Procedures and Investigations Act 1996 came into effect in April 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the prosecution of its own case (known as unused material) but disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by Section 5 of the Data Protection Act 2018 (known as subject access).

### 5.4 Freedom of Information Act 2000

If a request for images is received via a FOIA application and the person requesting is the subject, these will be exempt from the FOIA and will be dealt with under The Data Protection Principles and GDPR Articles. Any other requests not involving identification of individuals can be disclosed but only if it does not breach the data protection principles.

## 5.5 Investigatory Powers Act 2016

### Introduction

The Regulation of Investigatory Powers Act 2000 came into force on 2<sup>nd</sup> 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. It was updated in 2016 to include the types of errors and the reporting requirements, and how there is expected to be processes to identify if errors exist.

### Background

General observation forms part of the duties of many law enforcement officers and other public bodies. Police officers will be on patrol at football grounds and other venues monitoring the crowd to maintain public safety and prevent disorder. Officers may also target a crime "hot spot" in order to identify and arrest offenders committing crime at that location. Trading standards or HM Customs & Excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve **systematic surveillance of an individual**. It forms a part of the everyday functions of law enforcement or other public bodies. This low-level activity will not usually be regulated under the provisions of the 2016 Act.

Neither do the provisions of the Act cover the normal, everyday use of **overt** CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. However, it had not been envisaged how much the Act would impact on specific, targeted use of public/private CCTV systems by 'relevant Public Authorities' covered in Schedule 1: Part1 of the Act, when used during their planned investigations.

The consequences of not obtaining an authorisation under this Part may be, where there is an interference by a public authority with Article 8 rights (invasion of privacy), and there is no other source of authority, that the action is unlawful by virtue of section 6 of the Human Rights Act 1998 (Right to fair trial) and the evidence obtained could be excluded in court under Section 78 Police & Criminal Evidence Act 1984.

The Act is divided into five parts. Part II is the relevant part of the act for CCTV. It creates a system of authorisations for various types of covert surveillance. The types of activity covered are "intrusive surveillance" and "directed surveillance". Both types of surveillance if part of a pre-planned operation will require authorisation from specified persons named in the Act. In addition, the reasons for such surveillance must be clearly indicated and fall within the criteria outlined by this legislation.

A procedure is in place for regular reviews to be undertaken into authorisation. Any WMCA / Solihull / Walsall / Tamworth / East Staffordshire scheme will observe the criteria laid out in the legislative requirements. Further information is available from the Home Office website.

<b>Page: 17 of 44</b>	<b>Authority: M.Sayers</b>
<b>Date: February 2021</b>	

## **5.6 Surveillance Camera Code of Practice**

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

The code has been built upon 12 guiding principles, which provide a framework of good practice that includes existing legal obligations. Those existing obligations include the processing of personal data under the Data Protection Act 2018, a public authority's duty to adhere to the Human Rights Act 1998 and safeguards under the Regulation of Investigatory Powers Act 2000 associated with the use of directed and covert surveillance by a public authority. The use of a surveillance camera system must:

1. Always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
2. Take into account its effect on individuals and their privacy
3. Have as much transparency as possible, including a published contact point for access to information and complaints
4. Have clear responsibility and accountability for all surveillance activities including images and information collected, held and used.
5. Have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them.
6. Have no more images and information stored than that which is strictly required.
7. Restrict access to retained images and information with clear rules on who can gain access.
8. Consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Be subject to appropriate security measures to safeguard against unauthorised access and use.
10. Have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with.
11. Be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value, when used in pursuit of a legitimate aim.
12. Be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes.

Whilst the above principles are voluntary, Local Authorities must have regard to them and both WMCA and Walsall / Solihull / Tamworth / East Staffordshire Council's will work to achieve continued compliance with the requirements. Information and a copy of the Codes can be found [www.gov.uk](http://www.gov.uk)

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

Page: 18 of 44	Authority: M.Sayers
Date: February 2021	

### 5.7 Crime & Courts Act 2013

The Crime and Courts Act became law on 1<sup>st</sup> October 2013 and replaced the Serious Organised Crime and Police Act 2005. CCTV Control Rooms, RVRC's and the like are under Section 7 of the Crime & Courts Act 2013 required by law to share information (CCTV images) to the National Crime Agency (NCA). If a request is received from the NCA then the Redditch Borough Council and Bromsgrove District Council CCTV Control Room MUST comply with the request and provide the data.

*Section 7, Subsection (3)* provides information obtained by the NCA in connection with the exercise of any NCA function may be used by the NCA in connection with the exercise of any other NCA function. For example, information obtained in the course of gathering criminal intelligence may be used in connection with NCA's crime reduction function.

*Section 7, Subsection (4)* provides that the NCA may disclose information in connection with the exercise of any NCA function if the disclosure is for any "permitted purpose" as defined within Section 16(1) of the Act. This would apply in situations where, for example, the NCA has received information on suspected criminal activity (such as a 'Suspicious Activity Report' – which help banks and financial institutions protect themselves and their reputation from criminals and help law enforcement to track down and arrest them) and has decided to share this information with an organisation or person outside the NCA (such as a financial institution) for the purpose of preventing or detecting crime.

**NOTE: any information which falls within the scope of RIPA Act 2000 will still require the necessary authority prior to the release of images.**

## 6.0 ACCOUNTABILITY

### 6.1 Overview

WMCA and the Partners support the principle that the community at large should be satisfied that the Public surveillance CCTV systems are being used, managed and controlled in a responsible and accountable manner and that in order to meet this objective there will be independent assessment and scrutiny. It is the responsibility of all parties to maintain a continuous review of its integrity, security, procedural efficiency, methods of operation and retention and release of data in relation to the WMCA CCTV scheme.

### 6.2 Responsibilities

#### 6.2.1 The Owner

The owner(s) shall be responsible for policy, effective management and public relations of the scheme. They shall produce a written policy and be responsible for its implementation. This shall be carried out in consultation with users of the scheme and provide for the release of information relating to the operation of the system. The owner is responsible for dealing with complaints, and ensuring a fair system of staff selection and recruitment is adopted for staff employed in the control and monitoring environment. The role of owner also includes all statutory responsibilities including the role of “data controller” as prescribed by the Data Protection Act 2018.

#### 6.2.2 The Manager

The manager or designated member of staff should undertake regular reviews of the documented procedures to ensure that the provisions of this Code are being complied with. These should be reported back to the owner of the scheme. To facilitate this, regular minuted meetings will be held with the Supervisor to go through the points listed below:-

The manager is the person who has direct control of the scheme and as such he/she will have authority for the following

- Staff management
- Observance of the policy and procedural practices
- Release of data to third parties who have legal right to copies
- Control and security clearance of visitors
- Security and storage of data
- Security clearance of persons who request to view data
- Release of new and destruction of old data
- Liaison with police and other agencies
- Maintenance of the quality of recording and monitoring equipment

The manager should retain responsibility for the implementation of procedures to ensure that the system operates according to the purposes for which it was installed and in accordance with the objectives identified for the system.

Page: 20 of 44	Authority: M.Sayers
Date: February 2021	

The manager shall also ensure that on a day-to-day basis all equipment is working correctly and that the operators of the scheme comply with the Code of Practice and Procedural Manual. Dealing with breaches of the codes and disciplinary measures shall lie with the manager.

### 6.2.3 The Supervisor

The supervisor has a responsibility to ensure that at all times the system is operated in accordance with the policy and all procedural instructions relating to the system, and for bringing to the immediate attention of the manager any matter affecting the operation of the system, including any breach or suspected breach of the policy, procedural instructions, security of data or confidentiality. In the Managers absence the Supervisor will have responsibility for:

- Release of data to third parties who have legal right to copies
- Control and security clearance of visitors
- Security and storage of data
- Security clearance of persons who request to view data
- Release of new Media
- Liaison with police and other agencies

The supervisor should ensure that at all times operators carry out their duties in an efficient and responsible manner, in accordance with the objectives of the scheme. This will include regular checks and audit trails to ensure that the documentation systems in place are working effectively. These systems include:

- The media log
- The operator's log
- The incident log
- Witness statements
- Faults and maintenance log
- The security of data
- Audit logs
- Authorization of visitors – to be checked & counter signed by the team leader

The team leader should ensure operators comply with Health and Safety Regulations

### 6.2.4 The Operators

The operators are employed by the monitoring contractor and will be responsible for complying with the code of practice and procedural manual. They have a responsibility to respect the privacy of the individual, understand and comply with the objectives of the scheme. They are required to be proficient in the control and the use of the CCTV camera equipment, recording and playback facilities, image erasure, and maintenance of all logs.

The information recorded must be accurate, adequate and relevant to the purpose of the scheme. They should bring to the attention of the supervisor immediately any equipment defect that may occur.

Page: 21 of 44	Authority: M.Sayers
Date: February 2021	

In the Managers/Supervisors absence the Operator will have responsibility for:

- Release of data to third parties who have legal right to copies
- Control and security clearance of visitors
- Security and storage of data
- Security clearance of persons who request to view data
- Release of new Media
- Liaison with police and other agencies

#### 6.2.5 Contractor's Responsibilities

There is one contractor responsible for Maintenance of CCTV equipment and another separate contractor for the monitoring of the system. Both these elements are subject of a legal contract and contain performance requirements.

### 6.3 Accountability

The manager/supervisor shall be accountable to the owner of the scheme and will provide periodic progress reports on the scheme. The manager/supervisor will resolve technical and operational matters.

### 6.4 Annual Assessment

An annual assessment of the scheme will be undertaken by an independent consultancy appointed by the owner to evaluate the effectiveness of the system. This will include annual reviews of the scheme's operation, performance and working practices and, where appropriate make recommendations for improvements.

The results will be assessed against the stated purposes of the scheme. If the scheme is not achieving its purpose modification and other options will be considered. The results of the assessment will be made available through the WMCA organisation.

The Surveillance Camera Commissioner's CCTV Code of Practice stipulates that the system should be reviewed annually to determine whether CCTV continues to be justified. It further states that it is necessary to establish the system's effectiveness to ensure that it is still doing what it was intended to do. It is does not achieve its purpose, it should be stopped or modified.

The report should include the following;

- a) a description of the scheme and the geographical area(s) of operation;
- b) the scheme's policy statement;
- c) the objective and scope of the scheme;
- d) any changes to the operation or management of the CCTV scheme;
- e) any changes that have been made to the policy;
- f) any proposals to expand or reduce the operation of the scheme; and
- g) the scheme's aims and objectives for the next 12 months.

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

Page: 22 of 44

Authority: M.Sayers

Date: February 2021

The report should also provide details of the scheme's achievements during the previous 12 months, which might be based on information already held by the scheme. The details of the scheme's performance should include:

- 1) the number of incidents recorded by the scheme;
- 2) the number of incidents reported to the law enforcement agencies and, where appropriate, other bodies, e.g. the local authority;
- 3) an assessment of the scheme's impact on crime levels and types of crime in the area covered by it; and
- 4) an assessment of the scheme's impact on its objectives, including:
  - the number of privacy impact assessments completed;
  - the number of reviews of footage by police and authorized agencies; and
  - the number of incidents per camera for the previous twelve months.

### 6.5 Audit

Regular independent random audits will check the operation of the scheme and the compliance with the code of practice. It will consider the following:

- The level of attainment of objectives and procedures
- Random audits of the data log and release of information
- The review policy
- The complaints procedure

### 6.6 Complaints

A member of the public wishing to make a complaint about the system may do so through WMCA's complaint procedure. To make a complaint write to:

Customer Relations  
WMCA  
16 Summer Lane  
Birmingham  
B19 3SD

A complaints procedure has been documented. A record of the number of complaints or enquiries received will be maintained together with an outline of the action taken.

A report on the numbers of complaints will be collated by the systems manager or designated member of staff in order to assess public reaction to, and opinion of, the use of the system.

The annual report will contain details of the numbers of complaints received, the time taken to acknowledge and respond to complaints, the method of receiving and handling complaints and the degree of satisfaction in handling complaints.

## 6.7 Personnel

### 6.7.1 Security screening

All personnel employed to control/operate, audit, maintain or manage the scheme will be security screened in accordance with British Standard 7858 *Code of Practice for Screening of Personnel in a Security Environment*.

### 6.7.2 Training

WMCA consider that the thorough training of operatives is vital for the effective and efficient operation of the system. All operators are or will be trained to the criteria required by the private Security Industry Act 2001 and licensed by the Security Industry Authority for Public Space Surveillance systems. Training has also been undertaken in the following:

- Terms of employment
- The use of all appropriate equipment
- The operation of the systems in place
- The management of recorded material including requirements for handling and storage of material needed for evidential purposes.
- All relevant legal issues including Data Protection and Human Rights
- Progression to nationally recognized qualifications
- Recognise and understand privacy and disclosure issues
- The disciplinary policy

### 6.7.3 Contractors

There are special condition's imposed upon contractor's carrying out works on the system. These are detailed within the Procedural Manual.

## 7.0 CONTROL ROOM MANAGEMENT AND OPERATION

### 7.1 Access to Control Room

7.1.1 Access to the monitoring area will be strictly controlled. Security of the Control Room shall be maintained at all times.

7.1.2 Only those persons with a legitimate purpose will be permitted access to the control and monitoring room.

7.1.3 The Supervisor or in his/her absence the Deputy, is authorised to determine who has access to the monitoring area. This will normally be:

- (i) Operating staff
- (ii) The manager/Supervisor
- (iii) Police force employees requiring to view images, or collecting/returning media being considered for intelligence or evidential purposes. These visits will take place by prior appointment.
- (iv) Engineers and cleaning staff (These people will receive supervision throughout their visit).
- (v) Independent Inspectors appointed under this Code of Practice may visit the control room without prior appointment.
- (vi) Organised visits by authorised persons in controlled circumstances

All visitors to the monitoring area, including Police force employees, will be required to sign a visitor log and a declaration of confidentiality.

### 7.2 Response to an incident

7.2.1 The Procedural Manual details:

- What action should be taken
- Who should respond
- The time scale for response
- The times at which the observation should take place

7.2.2 A record of all incidents will be maintained in the incident log. Information will include anything of note that may be useful for investigative or evidential purposes.

### 7.3 Who makes the response and the time scale

Incidents of a criminal nature will be reported to the British Transport Police or West Midlands Police. The response will be made by the Police Service in accordance with their policies.

#### 7.4 Observation and recording of incidents

Recordings will be undertaken throughout a 24 hour period in digital format. In the event of an incident being identified there will be particular concentration on the scene and the operator will activate real time recording.

#### 7.5 A successful response

7.5.1 The criteria for measuring a successful response are:

- A good observational record of the incident
- A short time scale for response to the incident
- Identification of a suspect
- The prevention or minimisation of injury or damage
- Reduction of crime and disorder
- Improving public safety
- Restoration of tranquillity

#### 7.6 Operation of the System by the Police

- a) There is a monitor and control facility installed at specific Police Stations. Under certain circumstances the Police may make a request to monitor a number of cameras to which this Code of Practice applies. Following agreement by the control room supervisor at the time, the Police communications supervisor will provide sufficient information to the operator of the genuine requirement to monitoring only
  
- a) In the event of the police requesting use of the equipment from within the CCTV control room to monitor situations, such a request will only be permitted on the request of a police inspector or his designated deputy and only with the permission of the System manager or his designated deputy. The request should be in writing, however, in emergencies this can be a verbal request which should then be followed by the written request as soon as practicable. The monitoring room will continue to be staffed and equipment operated by, only those personnel who are authorised to do so and who fall within the terms of this Code.
  
- c) In very extreme circumstances such as a major incident a request may be made for the Police to take total control of the system in its entirety, including the staffing of the monitoring room and personal control of all associated equipment; to the exclusion of all representatives of the system owners. A request for total exclusive control must be made in writing by a Police Officer not below the rank of Superintendent (or designated deputy).

Once the police undertake any of the above they become responsible under the Data Protection Act 2018. A dedicated telephone link through to the police station is available to effectively relay information on incidents that arise.

## 8.0 PRIVACY AND DISCLOSURES ISSUES

### 8.1 Privacy

Cameras should not be used to infringe the individual's rights of privacy. The cameras generally are sited where they will not be capable of viewing any residential properties. If it is found there is a possibility that cameras would intrude in private areas, privacy zones would be programmed into the cameras where possible and CCTV operators trained to recognise privacy issues. The public address system should be moderated in volume and directed to the WMCA facility so as not to intrude into the space of neighbouring properties.

### 8.2 Disclosure Policy

8.2.1 The following principles must be adhered to:

- a) All employees will be aware of the restrictions set out in this Code of Practice in relation to access to, and disclosure of, recorded images.
- b) Images not required for the purposes of the scheme will not be retained longer than necessary. However, on occasions it may be necessary to retain images for longer period, where a law enforcement body is investigating a crime to give them the opportunity to view the images as part of an active investigation.
- c) The Data controller will only disclose to third parties who intend processing the data for the purposes registered with the Information Commissioner and which are deemed compatible with the objectives of the CCTV scheme.
- d) Monitors displaying images from areas in which individuals would have an expectation of privacy will not be viewed by anyone other than authorised employees of the user of the equipment.
- e) Recorded material will only be used for the purposes defined in the objectives and policy.
- f) Access to recorded material will be in accordance with policy and procedures.
- g) Information will not be disclosed for commercial purposes and entertainment purposes.
- h) All access to the medium on which the images are recorded will be documented.
- i) Access to recorded images will be restricted to those staff who need to have access in order to achieve the purpose(s) of using the equipment.
- j) Viewing of the recorded images should take place in a restricted area

8.2.2 Before data is viewed by a third party the manager should be satisfied that data is:

- a) The subject of a complaint or dispute that is unanswered
- b) The original data and the audit trail is maintained throughout
- c) Not part of a current criminal investigation by the Police, or likely to be so
- d) Not part of a civil proceeding or likely to be so
- e) Not removed or copied without proper authority
- f) The image obtained is aimed at identifying individuals or information relating to an individual.

### 8.3 Access to recorded images

Access to recorded images will be restricted to the manager or designated member of staff who will decide whether to allow requests for access by third parties in accordance with the disclosure policy.

### 8.4 Viewing recorded images

Viewing of recorded images should take place in a restricted area. Other employees should not be allowed to have access to that area when viewing is taking place

### 8.5 Operators

All operators are trained in their responsibilities in relation to access to privacy and disclosure issues.

### 8.6 Removal of medium for Viewing

The removal of medium on which images are recorded, for viewing purposes, will be documented in accordance with Data Protection principles and the procedural manual.

### 8.7 Access to data by third parties

8.7.1 Access to images by third parties will only be allowed in limited and prescribed circumstances. In the case of the WMCA CCTV scheme disclosure will be limited to the following:-

- a) law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- b) prosecution agencies
- c) legal representatives
- d) the media, where it is assessed by the Police that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. 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 (Data Subject) unless disclosure to an individual would prejudice the criminal enquiries or criminal proceedings.

8.7.2 All requests for access or for disclosure will be recorded. If access or disclosure is denied, the reason should be documented.

8.7.3 If access to or disclosure of the images is allowed, details will be documented.

8.7.4 Recorded images should not in normal circumstances be made more widely available, for example, they should not be routinely made available to the media or placed on the internet.

8.7.5 If it is intended that the images will be made more widely available, that decision should be made by the manager or designated member of staff and the reason documented.

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

<b>Page:</b> 28 of 44	<b>Authority:</b> M.Sayers
<b>Date:</b> February 2021	

- 8.7.6 The owner should not unduly obstruct a bona fide third party investigation to verify the existence of relevant data.
- 8.7.7 The owner should not destroy data that is relevant to previous or pending search request which may become the subject of a subpoena.
- 8.7.8 The owner should decide which other agencies, if any, should have access to data and it should be viewed live or recorded but a copy should never be made or released.

### **8.8 Disclosure in the public interest**

Requests to view personal data that do not fall within the above categories but that may be in the public interest should be considered. Examples may include public health issues, community safety or circumstances leading to the prevention or detection of crime. Material released to a third party for the purposes of crime prevention or detection, should be governed by prior written agreement with the relevant Chief Constable.

Material may be used for bona fide training such as Police or staff training.

### **8.9 Data subject access disclosure**

- 8.9.1 All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects and be aware of individual's rights under this section of the Code of Practice.
- 8.9.2 Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. This must be provided within a month of receiving a request.
- 8.9.3 Data subjects requesting access will be provided with a standard subject access request form (Appendix 'A') and accompanied leaflet (Appendix 'B') describing the types of images recorded and retained and the purposes for recording and retention.
- 8.9.4 Subject access rights are governed by Section 5 of the Data Protection Act 2018. They will include the following provisions:
- a) a person gives sufficient and accurate information about a time and place
  - b) information required as to the identification of the person making the request.
  - c) the Data Controller only shows information relevant to the search
- 8.9.5 If a copy is requested, it will be necessary to ascertain whether the images obtained are aimed at learning about the Data Subjects activities. If this is not the case and there has been no captured images of identifiable individuals or information relating to individuals then this may not fall within the Data Protection Act 2018 and access may be denied. Any refusal should be documented.

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

<b>Page:</b> 29 of 44	<b>Authority:</b> M.Sayers
<b>Date:</b> February 2021	

8.9.6 If on the other hand images have been obtain and CCTV used to focus on the activities of particular people either by directing cameras at an individual's activities, looking out for particular individuals or examining recorded CCTV images to find things out about the people in them such as identifying a criminal or a witness or assessing how an employee is performing. These activities will still be covered by the DPA and reference should be made to Section 8.2.2 of these Codes of Practice prior to the release of such data.

8.9.7 If images of third parties are also shown with the images of the person who has made the access request, consideration will be given as to whether there is a need to obscure the images of third parties. If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they should be obscured. In many cases, images can be disclosed as there will not be such intrusion.

8.9.8 The subject access request will be dealt with promptly and in any case within a month of receipt of the request or within a month of receiving all the information required.

8.9.9 All subject access requests should be dealt with by the manager or designated member of staff.

8.9.10 A search request should provide sufficient information to locate the data requested (e.g. within 30 minutes for a given date and place). If insufficient information is provided a data controller may refuse a request until sufficient information is provided.

8.9.11 Under certain circumstances (Section 112 and Schedule 11 Section 2 of the Data Protection Act 2018) the manager or designated member of staff can decide that a subject access request is not to be complied with. In such cases the refusal will be documented.

### **8.10 Provision of data to the individual**

The owner/manager having verified the validity of a request should provide requested material to the individual. Only that personal data specific to the search request should be provided. Other individuals should be blanked off by electronic screening or manual editing on the monitor screen. As there is no on site means of editing out other personal data the material would have to be sent to an editing house for processing. The procedure outlined in the CCTV Procedural Manual will be followed.

If the individual agrees it may be possible to provide subject access by viewing only. If this is the case:

- Viewing should take place in a controlled environment
- Material not relevant to the request should be masked or edited out

### **8.11 Other rights**

8.11.1 All staff involved in operating the equipment must be able to recognise a request from an individual exercising a data subject right (Chapter 3 Data Protection Act 2018).

8.11.2 In relation to a request to exercising a data subject right the manager or designated member of staff's response should indicate whether he or she will comply with the request or not.

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

Page: 30 of 44

Authority:

M.Sayers

Date: February 2021

8.11.3 The member or designated member of staff must provide a written response to the individual within 21 days of receiving the request setting out their decision on the request.

8.11.4 If the manager or designated member of staff decide that the request will not be complied with, they must set out their reasons in the response to the individual.

8.11.5 A copy of the request and response will be retained.

### **8.12 Media Disclosure**

Disclosure of images from the CCTV system must be controlled and consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet. Images can be released to the media for identification purposes; this will not generally be done by anyone other than a law enforcement agency.

## 9.0 RECORDED MATERIAL MANAGEMENT

**Images, which are not required for the purpose(s) for which the equipment is being used will not be retained for longer than is necessary. As mentioned previously, on occasions images may need to be retained for longer periods as a requirement of an investigation into crime. While images are retained access to and security of the images will be controlled in accordance with the requirements of the Data Protection Act and GDPR.**

- 9.1.1 Recorded material should be of high quality. In order for recorded material to be admissible in evidence total integrity and continuity must be maintained at all times.
- 9.1.2 Security measures will be taken to prevent unauthorised access to, alteration, disclosure, destruction, accidental loss or destruction of recorded material.
- 9.1.3 Recorded material will not be released to organisations outside the ownership of the system other than for training purposes or under the guidelines referred to previously.
- 9.1.4 Images retained for evidential purposes will be retained in a secure place where access is controlled.

### 9.2 Quality and Maintenance

In order to ensure that clear images are recorded at all times the equipment for making recordings and the associated security equipment including, where appropriate, help points and public address systems will be maintained in good working order with regular servicing in accordance with the manufacturer's instructions. In the event of a malfunction the equipment will be repaired within specific time scales which will be scheduled within the maintenance agreement. All documentation relating to the equipment and its servicing and malfunction is retained in the control room and will be available for inspection and audit.

### 9.3 Digital Recordings

In a digital CCTV system, the register should show the life of the recorded media at all stages whilst in the owner's possession. Such a register may also show itself to be useful in enabling evaluation of the CCTV scheme.

The register should include the following:

- 1) unique equipment reference number(s);
- 2) time/date/person removing medium from secure storage for use;
- 3) time/date/person returning medium to secure storage after use;
- 4) remarks column to cover additional points (e.g., erase/destroy/handed over to law enforcement agencies/removed from recording machine);
- 5) time and date of delivery to the law enforcement agencies, identifying the law enforcement agency officer concerned;
- 6) in the event of a non-automated system of erasure of data, the time/date/person responsible for erasure and/or destruction.
- 7) Details of all reviews of images, including persons present and results

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

<b>Page:</b> 32 of 44	<b>Authority:</b> M.Sayers
<b>Date:</b> February 2021	

9.3.1 Images will be retained for 31 days and unless containing evidence the medium will be destroyed.

9.3.2 Recorded material will be stored in a secure cabinet. Data to be destroyed will be destroyed as a controlled operation. Special consideration will be given to recorded material that has been requested by the Police or contains a known incident. This is covered within the Procedural Manual.

### **9.4 Making Recordings**

Details of the recording procedures are given in the Procedural Manual.

Recording mediums containing original incidents should not be replayed, unless absolutely essential to avoid any accident, damage or erasure. If recorded images need to be reviewed the reasons and details of those present will be logged and the medium returned to secure storage, if appropriate.

### **9.5 Prints**

Prints will only be made when absolutely necessary. All prints will remain the property of the scheme owner and those not handed to the police will be retained in a secure cabinet until destruction is authorised. The taking of prints will be recorded in a register to be retained in the control room.

## 10.0 DOCUMENTATION

### 10.1 General

All documentation will be computerised and auditable.

### 10.2 Logs

An accurate log of operator working times will be maintained. Each operator will maintain a log of any event or occurrence including:

- a) change of operator identifying the operator on duty at that workstation and showing that:
  - the necessary recording material has been loaded in the correct recording equipment
  - that the correct time was being displayed
  - that the recording equipment appeared to be operating correctly
- b) incidents including details of time, date, location, nature, name of operator dealing and action taken
- c) routine camera patrols, whether taken manually or through the utilisation of pre-set times
- d) Privacy zones, detailing where, for any reason, it is necessary to encroach on private areas that are not part of the contractual patrol
- e) help point activity
- f) public address use

### 10.3 Administrative documents

The following documentation will be maintained on a computerised programme:

- digital tracking record
- occurrence/incident record
- maintenance of equipment, whether routine or breakdown record
- print log
- list of installed equipment

In addition, the following will also be available

- visitors register
- staff signing on and off duty

<b>Page: 34 of 44</b>	<b>Authority: M.Sayers</b>
<b>Date: February 2021</b>	

**Appendix 'A'**

**Subject Data Access Form**

**How to Apply for Access to Information Held on the CCTV System**

These notes explain how you can find out what information, if any, is held about you on the CCTV System.

**Your Rights**

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 the information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or data does not fall within the Data Protection Act 2018 or if you agree otherwise. WMCA will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the WMCA is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

**WMCA CCTV System Rights**

WMCA may deny access to information where the Act allows or does not apply. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders
- Where the Data protection Act 2018 does not apply (Durant –v- FSA (2003))

And giving you the information may be likely to prejudice any of these purposes.

**THE APPLICATION FORM: (N.B. ALL sections of the form must be completed. Failure to do so may delay your application.)**

**Section 1** - Asks you to give information about yourself that will help us confirm your identity. We have a duty to ensure that information it holds is ensure and it must be satisfied that you are who you say you are.

**Section 2** - Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full photograph of you.

**Section 3** - The declaration must be signed by you.

**When you have completed and checked this form, take or send it together with the required TWO identification documents, photograph and fee to:**

Customer Relations  
 WMCA  
 16 Summer Lane  
 Birmingham  
 B19 3SD

**CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES**

<b>Page:</b> 35 of 44	<b>Authority:</b> M.Sayers
<b>Date:</b> February 2021	

**SECTION 1 About Yourself**

The information requested below is to help us (a) satisfy itself as to your identity and (b) find any data held about you.

PLEASE USE BLOCK CAPITAL LETTERS

<b>Title</b> ( <i>tick box as appropriate</i> )	Mr	<input type="checkbox"/>	Mrs	<input type="checkbox"/>	Miss	<input type="checkbox"/>	Ms	<input type="checkbox"/>
<b>Other title</b> ( <i>e.g. Dr., Rev., etc.</i> )								
<b>Surname/family name</b>								
<b>First names</b>								
<b>Maiden name/former names</b>								
<b>Sex</b> ( <i>tick box</i> )	Male	<input type="checkbox"/>	Female	<input type="checkbox"/>				
<b>Height</b>								
<b>Date of Birth</b>								
<b>Place of Birth</b>	Town							
	County							

<b>Your Current Home Address</b> <i>(to which we will reply)</i>								
	Post Code							
	Tel. No.							
A telephone number will be helpful in case you need to be contacted.								

*If you have lived at the above address for less than 10 years, please give your previous addresses for the period:*

<b>Previous address(es)</b>								
<b>Dates of occupancy</b>	From:				To:			
<b>Dates of occupancy</b>	From:				To:			

CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

Page: 36 of 44

Authority:

M.Sayers

Date: February 2021

**SECTION 2 Proof of Identity**

To help establish your identity your application must be accompanied by TWO official documents that between them clearly show your name, date of birth and current address.

For example: a birth/adoption certificate, driving license, medical card, passport or other official document that shows your name and address.

Also, a recent, full face photograph of yourself.

**Failure to provide this proof of identity may delay your application.**

**SECTION 3 Supply of Information**

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:

(a) View the information and receive a permanent copy

(b) Only view the information

**SECTION 4 Declaration**

**DECLARATION** (to be signed by the applicant)

The information that I have supplied in this application is correct and I am the person to whom it relates.

Signed by

Date

**Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.**

**NOW – please complete Section 4 and then check the ‘CHECK’ box (on page 5) before returning the form.**

CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

Page: 37 of 44	Authority: M.Sayers
Date: February 2021	

**SECTION 5 To Help us Find the Information**

If the information you have requested refers to a specific offence or incident, please complete this Section.

Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet, in the same way, if necessary.

If the information you require relates to a vehicle, property, or other type of information, please complete the relevant section overleaf.

Were you: (tick box below)

<i>A person reporting an offence or incident</i>	<input type="checkbox"/>
<i>A witness to an offence or incident</i>	<input type="checkbox"/>
<i>A victim of an offence</i>	<input type="checkbox"/>
A person accused or convicted of an offence	<input type="checkbox"/>

Other – please explain


Date(s) and time(s) of incident	
Place incident happened	
Brief details of incident	

CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

Page: 38 of 44

Authority: M.Sayers

Date: February 2021

**Before returning this form**

- Have you completed ALL Sections in this form?

**Please check:**

- Have you enclosed TWO identification documents?
- Have you signed and dated the form?

**Further Information:**

These notes are only a guide. The law is set out in the Data Protection Act 2018, obtainable from The Stationery Office. Further information and advice may be obtained from:

**The Office of the Information Commissioner,  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF.  
Tel. (01625) 545745**

Please note that this application for access to information must be made direct to **WMCA** (address on Page 1) and **NOT** to the Information Commissioner.

**OFFICIAL USE ONLY**

**Please complete ALL of this Section (refer to 'CHECK' box above).**

Application checked and legible?

Date Application Received

Identification documents checked?

Details of 2 Documents (see page 3)

Documents Returned?

**Member of Staff completing this Section:**

Name

Location

Signature

Date

**Appendix 'B'**

**CCTV SCHEME LEAFLET**

**The Data Protection Act 2018**

**CCTV IN OPERATION**

**This brochure contains advice and information regarding data recorded by the CCTV system and gaining access to that data.**

WMCA  
16 Summer Lane  
Birmingham  
B19 3SD

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

Page: 40 of 44

Authority:

M.Sayers

Date: February 2021

### THE PURPOSES FOR WHICH IMAGES ARE RECORDED

Full details of the principles and criteria under which this system operates may be found in the CCTV Code of Practice. The aims and key objectives of the system are:

#### **Purpose Description:**

This Purpose Includes:

Further description Initiatives Under the Crime and Disorder Act 1998.

Executive Premises Where the Object Is the Prevention and Detection of Crime Community Safety Programmes

Operation of CCCTV Systems in Public Space:

Includes Use of Closed-Circuit Television for The Monitoring and Collection of Sound And/Or Visual Images for The Purpose of Maintaining

The Security of Premises, For Preventing Crime and Investigating Crime and Operational Management. Health and Safety Management.

Business Administration Including Bus Stations, Rail Stations, Tram Network, Park and Ride Sites, Residential Dwellings, Bus Shelters and For the Purpose of Monitoring Operational Activities to Include Passenger Flows, Bus Movements and Problem.

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

Page: 41 of 44

Authority:

M.Sayers

Date: February 2021

### WMCA

### CCTV SCHEME

### CODE OF PRACTICE

Copies of the Code of Practice are available free of charge on application to the CCTV System Manager.

### **RECORDED IMAGES**

The storage, processing and use of the recorded data obtained by the CCTV system is guided by the following general principles.

Recorded data will only be used for the purposes defined in the Code of Practice and in accordance with the provisions of the Data Protection Act and Human Rights Act.

Access to recorded data shall only take place in the circumstances defined in the Code of Practice and the provisions of the relevant legislation.

Recorded data will not be sold or used for commercial purposes or the provision of entertainment.

The showing of recorded data to the public will only be permitted in accordance with the law in relation to the investigation, prosecution or prevention of crime.

Data released shall remain the property of WMCA.

## CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES

Page: 42 of 44	Authority: M.Sayers
Date: February 2021	

### DISCLOSURE POLICY

Disclosure of data obtained by the CCTV System will only be committed in accordance with the relevant legislation and the criteria contained within the Code of Practice.

In every case a written application in an approved format, clearly showing the reasons for the request is required.

The code lists third parties from who requests to view data will be regarded as 'primary requests' and sets out circumstances in which such applications may be made.

Third parties include:

The Police; Fire Service; H.M. Customs & Excise; WMCA (Specific Officers); Other statutory prosecuting bodies (e.g. Trading Standards, Ministry of Defence Police; British Transport Police; etc); solicitors; plaintiffs/defendants and persons exercising their rights of subject access under the Data Protection Act 2018.

### SUBJECT ACCESS

If you wish to exercise your rights of subject access as provided for in the Data Protection Act 2018 you will be required to make the request in writing on a standard subject access request form.

All requests for subject access will be dealt with by the CCTV Manager or a nominated deputy. A written response to the request will be provided within a month of receipt, either setting out the steps intended to take to comply with the request or setting out the reason for refusing the request.

The CCTV Systems. A copy of this code may be obtained on application to the Data Protection Commissioner.

**CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES**

**Page: 43 of 44**

**Authority:**

**M.Sayers**

**Date: February 2021**

**Appendix 'C'**

***Agreed by***

**WMCA**

***And***

**Man Commercial Protection LTD**

***And***

**West Midlands Police**

***And***

**British Transport Police**

***Certificate of Agreement***

**CODE OF PRACTICE FOR THE WMCA CCTV SCHEMES**

<b>Page: 44 of 44</b>	<b>Authority: M.Sayers</b>
<b>Date: February 2021</b>	

*The content of both this Code of Practice and the Procedural Manual are hereby approved in respect of the WMCA 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 WMCA**

Signature: .....

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

Dated the ..... day of .....

**Signed on behalf of Man Commercial Protection LTD**

Signature.....

Name..... Position Held.....

Dated the..... day of.....

**Signed for and on behalf of Police Area Commander West Midlands Police**

Signature: .....

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

Dated the ..... day of .....

**Signed for and on behalf of Police Area Commander British Transport Police**

Signature: .....

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

Dated the ..... day of .....