

# **CCTV**

# **Code of Practice**



**MANCHESTER**  
**CITY COUNCIL**

[www.manchester.gov.uk](http://www.manchester.gov.uk)

## Document Control

Title	Manchester City Council – CCTV Code of Practice
Document Type	
Author	K Rennicks
Owner	CCTV Team
Subject	Closed Circuit Television System
Protective marking	
Created	27 June 2008
Review due	2028 or earlier where there is a change in the applicable law, official guidance or a Council restructure affecting this Guidance

## Revision History

Version	Date	Author	Description of change
v.1.1	27.06.08	K Rennicks	
v.1.2	11.03.13	D Holden, CCTV Manager	3.3 amendment to paragraph on data subject access requests
v.2.0	September 2019	Ian Mark Principal Lawyer, Democratic Services Legal	Policy updated to reflect Home Office Surveillance Camera Code of Practice and updated ICO Data Protection Code of Practice for surveillance cameras and personal information (May 2015)
v.3.0	November 2021	Ian Mark, Principal Lawyer. Democratic Service Legal	Policy updated to revise clause 5 to reflect change in GMP access to CCTV system and to take account of minor changes to the title of legislation, procedure and typographical errors
v.4.0	April 2026	Democratic Services Legal	Code of Practice updated to add new clause 3.3.3 and to take account of changes to legislation, guidance and the updated Home Office Surveillance Camera Code of Practice. Clause 9.10 inserted as reference to the Council's RIPA policy. Other minor changes to clarify legislation, procedures or updates to external terminology.

## TABLE OF CONTENTS

1.	INTRODUCTION .....	5
2.	OBJECTIVES OF USING CCTV CAMERAS .....	5
3.	STATEMENT OF PURPOSE AND PRINCIPLES .....	6
4.	ACCOUNTABILITY AND PUBLIC INFORMATION .....	8
5.	OPERATION OF THE SYSTEM .....	9
6.	MANAGEMENT OF FOOTAGE .....	11
7.	REQUESTS BY INDIVIDUALS FOR CCTV FOOTAGE (DATA SUBJECT ACCESS REQUEST) .....	13
8.	REQUESTS BY THIRD PARTIES FOR CCTV FOOTAGE.....	15
9.	REQUESTS FOR CCTV FOOTAGE BY MANCHESTER CITY COUNCIL STAFF FOR INTERNAL WORK RELATED PURPOSES .....	17
10	ASSESSMENT AND REVIEW.....	17
10.1	ANNUAL REVIEW .....	17
11.	INFORMATION AND COMPLAINTS .....	18
12.	DISCIPLINARY ACTION AGAINST COUNCIL STAFF .....	19
	APPENDIX 1 DATA PROTECTION PRINCIPLES .....	20
	APPENDIX 2 SURVEILLANCE CODE GUIDING PRINCIPLES.....	21
	APPENDIX 3 TEMPLATE REPORT .....	24



## **1. INTRODUCTION**

- 1.1 Manchester City Council operates CCTV cameras within Manchester's public areas (public area cameras) and within and around its premises (premises cameras).
- 1.2 The public area cameras cover public areas in the City Centre, other district centres and public open spaces and are operated from a secure central control room where the images are monitored and recorded. The public area cameras may also be operated from the Council's Emergency Control Centre. A general description of the locations of the Council's public area cameras can be found at [CCTV Cameras and Security](#).
- 1.3 Premises cameras are standalone systems that cover separate Council premises and will be operated in a secure environment where the images can be monitored and recorded.
- 1.4 Public area and some premises cameras operate in colour and have pan, tilt and zoom capabilities, which means they can scan areas, focus in on people (and objects) and follow them. These cameras do not record sound.
- 1.5 The Council may also record footage using:
  - body worn cameras (which may also record sound)
  - mobile cameras mounted in Council vehicles
  - automatic number plate recognition cameras
- 1.6 CCTV cameras and monitoring and recording equipment are owned by the Council but may be operated by contractors as well as Council staff.
- 1.7 This Code of Practice does not apply to schools in the Manchester City Council area as schools are data controllers in their own right.

## **2. OBJECTIVES OF USING CCTV CAMERAS**

- 2.1 The Council's objectives in using CCTV cameras are:
  - To increase safety for those people who live, work, trade within and visit Manchester including monitoring for security and safety purposes of Council staff and visitors in Council premises.
  - To assist in the deterrence and detection of crime (including environmental crime), disorder and anti-social behaviour in Manchester; and in the upholding of legal rights. This will include:
    - Helping to identify, apprehend and prosecute offenders

- Providing evidence for criminal and civil action in the courts including preliminary investigation of claims
- Countering terrorism
- To help reduce the fear of crime and provide reassurance to the public
- To increase safety for those people who live, work, trade within and visit Manchester including monitoring for security and safety purposes of Council staff and visitors in Council premises
- To assist in the overall management of public places
- To assist in developing the economic wellbeing of the Manchester area and encourage greater use of the City Centre
- To assist the Council in carrying out its regulatory functions in relation to environmental health and protection, pollution control, contaminated land, health and safety, food safety, animal welfare, consumer protection, weights and measures and licensing.
- To provide traffic management support and enforce bus lane and parking restrictions
- To provide assistance and direction in the event of a major emergency in Manchester

### **3. STATEMENT OF PURPOSE AND PRINCIPLES**

#### **3.1 Purpose of this Code**

3.1.1 The purpose of this Code is to outline how the Council uses CCTV cameras to meet its objectives in accordance with the relevant legislation and guidance.

#### **3.2 General Principles of Operation**

3.2.1 The Council is committed to safeguarding the rights of people visiting, living and working in Manchester. The Council will ensure that the cameras are operated in accordance with the principles in:

- (a) [The Human Rights Act 1998](#)
- (b) The UK General Data Protection Regulation and the [Data Protection Act 2018](#) ('data protection legislation') (see the data protection principles in Appendix 1).
- (c) [The Home Office Surveillance Camera Code of Practice](#) prepared in accordance with sections 29 to 31 of the Protection of Freedoms Act 2012 (the Surveillance Code) (see the Guiding Principles in Appendix 2)

- (d) [The Information Commissioner's guidance-on-video-surveillance-including-cctv](#) (the ICO code)
- (e) The [Regulation of Investigatory Powers Act 2000](#)
- (f) The [Freedom of Information Act 2000](#)/ Environmental Information Regulations 2004
- (g) The Equality Act 2010

3.2.2 CCTV cameras will be operated fairly, within the law, and only in so far as is necessary to achieve the purposes for which they are currently used and which are set out in this Code, or which are subsequently agreed in accordance with this Code.

3.2.3 Any other organisation, individual, including Council staff, or authority participating in the operation of the CCTV cameras or accessing footage provided by the CCTV cameras must comply fully with this Code and with any contractor's operational guidelines approved by the Council.

### **3.3 Monitoring by Council CCTV Managers**

3.3.1 The Council's CCTV Managers (or such other officers as have the day to day management of a CCTV control room or secure operating environment (CCTV Control Rooms) and CCTV footage, irrespective of their title but referred to in this Code of Practice as CCTV Managers) have unrestricted access to the CCTV Control Rooms and receive regular reports as and when required from the Council's contractors.

3.3.2 The Council's CCTV Managers have day-to-day responsibility for the monitoring and operation of the Council's CCTV cameras and the implementation of this Code.

3.3.3 In exceptional circumstances certain designated officers other than a Council CCTV Manager will be entitled to access CCTV footage. This would only be permissible when the CCTV Manager is not on site and uncontactable and footage needs to be viewed immediately to establish the facts relating to an emergency situation which gives rise to a risk to someone's health and safety. The designated officer will retain a password for use in such situations. Any such access is to be logged and a job raised retrospectively via the Council's helpdesk to ensure it is included in the Annual Review referred to in 10.1. Where the footage is subsequently required the normal process around disclosure and archiving is to be followed.

3.3.4 The Council's CCTV Managers report on a yearly basis (or sooner in respect of specific issues requiring more immediate consideration) to the relevant Directorate

Senior Information Risk Officer ('DSIRO') with responsibility for their CCTV cameras. The template report at Appendix 3 shows the items to be covered.

### **3.4 Copyright**

3.4.1 Copyright and ownership of all footage recorded from the CCTV cameras will remain with the Council. However, once there has been disclosure of footage to another body such as the police then the recipient becomes responsible for their copy of that footage and must comply with all applicable legal obligations. Disclosure of footage is addressed further in sections 7, 8 and 9 of this Code.

### **3.5 Processing and Handling of Footage**

3.5.1 No footage will be released, including that requested by Council staff for internal work-related purposes, except in accordance with either section 7, 8 or 9 of this Code.

### **3.6 Breach of this Code of Practice**

3.6.1 If the Council fails to comply with this Code of Practice, the validity of properly imposed fines, penalty charge notices or other financial penalties issued by the Council shall not be affected.

## **4. ACCOUNTABILITY AND PUBLIC INFORMATION**

### **4.1 The Public**

4.1.1 The Surveillance Code is clear that individuals and the public must have confidence that CCTV cameras are deployed to protect and support them rather than to spy on them. The use of overt surveillance in a public place which is in pursuit of a legitimate aim, meets a pressing need must also consider the effect on individuals and their rights under the HRA and data protection legislation. Public confidence is dependent on the Council operating the CCTV cameras lawfully and in a transparent and accountable manner. The Council has therefore established procedures for requesting information and making complaints so that it can keep the public fully informed about the operation of the Council's CCTV cameras. See Section 11 for more details.

### **4.2 Signage**

4.2.1 Signs will be prominently placed to advise people that CCTV cameras (including those used for automatic number plate recognition (ANPR)) are in operation. The signs will indicate:

- (i) the presence of CCTV monitoring;
- (ii) who is responsible for the cameras; and

(iii) the contact telephone number or e-mail address for the Council (unless this is dangerous or impracticable, for example on ANPR cameras).

4.2.2 In the case of body worn cameras, persons wearing them will have signs displayed on their uniforms informing people that footage may be recorded and will also advise people that they are about to be filmed.

4.2.3 In the case of mobile cameras on CCTV cars, the cars have signs on them alerting the public that they record using CCTV cameras and they only operate in areas where CCTV signage is in place.

### **4.3 Published Information**

4.3.1 A copy of this Code of Practice will be published on the Council's website.

## **5. OPERATION OF THE SYSTEM**

### **5.1 Staff**

5.1.1 The Council will ensure that CCTV Control Rooms are staffed by specially selected and trained operators in accordance with the requirements of the Private Security Industry Act 2001. The Council will also ensure that staff are aware of quality management and competency standards produced by the Biometric and Surveillance Camera Commissioner and are trained in respect of all legislation appropriate to their role, including a comprehensive induction process. Operational procedures ensuring the security and integrity of the CCTV cameras' use will be approved by the Council and kept up to date.

5.1.2 The Council will ensure that all relevant staff members are aware of its rules, policies and procedures relating to operation of the CCTV cameras including this Code, the ICO code and the Surveillance Code.

5.1.3 The Council will ensure that staff are aware that the CCTV cameras must be operated fairly and without discrimination based on personal prejudice; and not for personal reasons or personal curiosity. Staff may be asked to justify their interest in, or recording of, a particular piece of footage as part of regular audits.

### **5.2 Declaration of Confidentiality**

5.2.1 Every person required to comply with the terms of this Code and who has any involvement with the operation of the CCTV cameras, will be required to sign a declaration of confidentiality. Visitors, including Council staff, to a CCTV Control Room must establish they have a lawful, proper, and sufficient reason to enter the Control Room and will also be required to confirm in writing that they accept a duty of confidentiality (see paragraph 5.3.2 below)

### **5.3 Access to and Security of the CCTV Control Rooms and Associated Equipment**

5.3.1 Signals from the public area CCTV cameras and certain key Council buildings are received in the CCTV Control Rooms where they are relayed onto various monitors. For reasons of security and confidentiality, access to the CCTV Control Rooms is restricted to authorised personnel only. Public access to the CCTV Control Rooms and recording facility is prohibited except for lawful, proper and sufficient reasons. Any such visits will be conducted and recorded in accordance with the contractor's operational rules, procedures and guidelines approved by the Council. In relation to the other premises cameras appropriate measures will be put in place to ensure security and confidentiality.

5.3.2 Regardless of their status, all visitors to a CCTV Control Room, including inspectors and auditors, will be required to confirm in writing that they have read and accept the terms of entry to the CCTV Control Room (including the need to maintain confidentiality).

5.3.3 Authorised personnel will normally be present at all times when the equipment in a CCTV Control Room is in use. If a CCTV Control Room is to be left unattended for any reason it will be secured. In the event of a CCTV Control Room being evacuated for safety or security reasons, the emergency procedures in the approved operational guidance will be followed.

### **5.4 Control and Operation of Cameras**

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

#### **5.4.2 Control**

5.4.2.1 Control of the CCTV cameras lies only with those trained and authorised staff with responsibility for using the CCTV cameras, including control equipment and recording and reviewing equipment, except where special arrangements are agreed with the police as in paragraph 5.4.3 below.

#### **5.4.3 Operation of the System by the Police**

5.4.3.1 The police may make a request to direct CCTV cameras under the Regulation of Investigatory Powers Act 2000. Only requests made on the written authority of a police authorising officer of Superintendent rank or above will be considered. If the urgency of the situation makes a written request impracticable, a verbal request from a police officer of any rank may be made. Any such request will be complied with, or not, at the discretion of the relevant CCTV Manager, or their designated deputy, and a record kept of that decision.

- 5.4.3.2 If a request from the police is accepted, the relevant CCTV Control Room will continue to be staffed and equipment operated by only those staff who are authorised to do so, who will operate the CCTV cameras under the direction of the police officer designated in the written authority or who has made the verbal request; unless the written authority requests that the CCTV cameras be operated by a designated police officer and the relevant CCTV Manager has agreed to this.
- 5.4.3.3 In very extreme circumstances a request may be made by the police to take total control of CCTV cameras, including staffing the relevant CCTV Control Room and taking personal control of all associated equipment, to the exclusion of all staff of the Council and its contractor. Any such request must be made to the relevant CCTV Manager in the first instance, who will consult personally with the relevant Directorate Senior Information Risk Officer (DSIRO) with responsibility for their CCTV Control Room. A request for total exclusive control must be made in writing by a police officer of the rank of Assistant Chief Constable or above. If the urgency of the situation makes a written request impracticable, a verbal request may be made by a police officer of that rank or above.
- 5.4.3.4 A number of designated GMP officers in the Silver Command Control room, the City Centre policing team and associated radio operators are also able to view all CCTV cameras in the City Centre independently of a Council CCTV operator. In addition to being able to view a camera those GMP officers also have the ability to use the pan, tilt, and zoom features of all cameras they have access to. All such viewing and also use of the features of the CCTV cameras is controlled through a single generic user account and GMP keep records to show which individual officers are using the CCTV cameras at any time. Representatives of the Council, and other Greater Manchester partners such as the Greater Manchester Fire & Rescue Service and the North West Ambulance Service also have access to view the CCTV feedback when working in the Silver Command Control room. Nothing in this paragraph overrides the requirements set out in 5.4.3.1, 5.4.3.2 or 5.4.3.3 above.

#### **5.4.4 Secondary viewing**

- 5.4.4.1 Facilities to view live footage are provided at secondary locations accessed by Manchester City Council Civil Contingencies Officers, Greater Manchester Police (GMP) and by Transport for Greater Manchester (TfGM). TfGM have the ability to change the direction the cameras face.

## **6. MANAGEMENT OF FOOTAGE**

### **6.1 Guiding Principles**

- 6.1.1 The Council and its contractors will operate the CCTV cameras with regard to the guidance in the ICO Code for looking after footage from the CCTV cameras and using the information contained in it. In this Code footage means anything recorded

from the CCTV cameras, including digitally recorded footage. All footage obtained through using the CCTV cameras has the potential for containing material that may need to be admitted in court as evidence.

6.1.2 The public must have total confidence that information recorded about their ordinary every day activities will be treated with due regard to their right to respect for their private and family life. The Council will therefore, irrespective of the format (e.g. paper copy, CD, DVD, or any form of electronic processing and storage) of the footage obtained from the CCTV cameras, treat it strictly in accordance with this Code from the moment it is received by the CCTV Control Room until final destruction. Every movement and usage will be meticulously recorded.

6.1.3 Access to and the use of footage will be strictly for the purposes defined in this Code. Footage will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

6.1.4 Footage may be released for the purposes of identification on a case by case basis where considered proportionate and necessary and as permitted by law.

## **6.2 Recording Policy**

6.2.1 Subject to the equipment functioning correctly, images from every camera will be recorded on a continuous basis.

## **6.3 Retention**

6.3.1 Where practicable all digital recording will be set to overwrite automatically at the end of the 31 day retention period. Footage may, however, be retained for longer than the usual 31 days if required, or appears likely to be required, for evidential purposes in accordance with the provisions of this Code. The appropriate additional retention period will be decided on a case by case basis by the relevant CCTV Manager. Where automatic overwrite is not practicable a manual overwrite will be actioned at the end of the 31 day retention period.

## **6.4 Record of use of footage**

6.4.1 A record of all use of footage will be kept, showing each occasion on which that footage has been accessed, retrieved, recorded, viewed or disclosed. Where footage is released in accordance with this Code, a record will be kept which identifies the basis for that release, and to whom. These records will be retained for at least **three** years.

## **6.5 Storage of footage**

6.5.1 Footage is stored in a way that maintains the integrity of the information contained in it. CCTV footage is stored on secure servers in secure areas with limited access

authorities in place. Only authorised staff may access the footage using individual logons and passwords to access the system.

## **6.6 Prints from footage**

6.6.1 Prints will be treated in the same way as footage. They will only be released as permitted by this Code, and any release will be recorded.

6.6.2 Where prints which contain personal images, are taken for use within the CCTV control centre, they should not be kept for longer than can be reasonably justified and should be regularly reviewed. Prints that are no longer required will be securely destroyed.

## **7. REQUESTS BY INDIVIDUALS FOR CCTV FOOTAGE (DATA SUBJECT ACCESS REQUEST)**

7.1. The use of the CCTV cameras and footage captured from them will comply with the data protection principles contained in the UK General Data Protection Regulation and Data Protection Act 2018 which are set out in Appendix 1.

### **7.2 Requests for CCTV footage containing images of individuals requesting footage**

7.2.1 The Council and its contractors will have regard to [the ICO's guidance-on-video-surveillance-including-cctv](#) relating to CCTV and requests for images captured by CCTV cameras. To request access to CCTV images, applicants can visit the following webform: [www.manchester.gov.uk/cctvrequest](http://www.manchester.gov.uk/cctvrequest). Requests can also be made in writing, by post, or email to the addresses set out in section 11.1 or orally by contacting any officer of the Council or an officer of its contractor.

7.2.2 Images of people obtained from CCTV cameras are their personal data and they have the right to be given a copy of the CCTV footage containing their images, subject to certain exemptions. The most likely exemptions are where releasing the footage would be likely to prejudice:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of any tax or duty or of any imposition of a similar nature

Any exemptions will be considered on a case by case by the Council.

7.2.3 The webform asks for the following information:

- The date and approximate time (to the nearest 15 minutes) of the incident in relation to which the CCTV footage is requested
- The location and direction of travel of the person in the footage at the time of the incident
- Details of any vehicle in which the person in the footage was travelling at the time of the incident
- A description of the clothing worn by the person in the footage at the time of the incident, including details of any distinctive colours, markings or materials
- Whether the CCTV footage is likely to include images of other people

7.2.4 The Council will **not** be permitted to charge a fee for providing the footage unless it determined the request is manifestly unfounded or excessive. If a fee is charged it must reflect the administrative costs of providing, communicating the information or taking action as requested.

7.2.5 Requests received will be logged by the Democratic Services Information Compliance Group (Infocompliance Group).

7.2.6 The Council normally destroys CCTV footage after 31 calendar days. Upon receipt of the request, the Info compliance Group will arrange for the CCTV footage to be retained while waiting for the documents referred to in paragraph 7.2.8 below. Requests will still be made to establish if the CCTV footage exists even if the date of the incident was more than 31 days ago.

7.2.7 Where appropriate, the Infocompliance Group will write to the applicant requesting the following:

- Two forms of proof of photographic identity, including confirmation of the current address of the person asking for footage
- A signed letter of authority (if the request is being made through an agent such as a solicitor or insurance company)
- A recent photograph of the person who is making, or on whose behalf, the request is being made

7.2.8 People asking for footage will be advised of the 31 day retention period for CCTV footage and that the relevant CCTV Manager has been requested to keep any footage until receipt of the documents and fee (where appropriate). CCTV footage requested to be retained is kept for a period of six months.

- 7.2.9 If the CCTV Manager is able to locate the requested footage then they will provide a reference number to the Infocompliance Group which will enable the footage to be matched to the request when the documents are received.
- 7.2.10 If it is confirmed that no CCTV footage exists, the Infocompliance Group will inform the person asking for footage or their agent.
- 7.2.11 If it has been established that CCTV footage is held and more than three months have passed without the person asking for the footage providing the documents, then the requested footage will be kept on hold for three months after which the footage will no longer be retained.
- 7.2.12 When all the documents have been provided and where required, a fee paid, the CCTV team will copy the footage on to a disc which will be provided to the relevant CCTV Manager. They will view the footage to consider if it is appropriate to release it in accordance with the person's data subject rights under data protection law.
- 7.2.13 If the footage is to be released then it will be sent to the person asking for the footage on an encrypted disc by recorded delivery or to provided via secure format electronically or some other secure method. The encryption key is sent separately.
- 7.2.14 Images of other identifiable individuals in the footage or their personal data such as their vehicle number plates will be pixelated.

## **8. REQUESTS BY THIRD PARTIES FOR CCTV FOOTAGE**

### **8.1. General principles**

- 8.1.2. Every request for the release of personal images generated by CCTV cameras will be referred to the relevant CCTV Manager or his/her representative.
- 8.1.3 The Council will, as far as reasonably practicable, safeguard people's right to privacy and ensure that footage is disclosed to third parties lawfully and fairly in accordance with the provisions of the Freedom of Information Act 2000, the Human Rights Act 1998 and the UK General Data Protection Regulation and Data Protection Act 2018.
- 8.1.4 Members of GMP or other agency having a statutory authority to investigate and/or prosecute offences may, subject to compliance with this Code, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses or to trace the whereabouts of a missing person as a matter of urgency.
- 8.1.5 Where footage is provided to GMP or other agency having a statutory authority to investigate and/or prosecute offences, GMP or that other agency will take full

responsibility for their use of that footage and will be considered a controller, (as defined under data protection legislation), for any personal data they process.

## **8.2 Requests for CCTV footage**

8.2.1 Requests to disclose footage generated by the CCTV cameras may be made by third parties for any one or more of the following purposes:

- Providing evidence in criminal proceedings
- Providing evidence in civil proceedings or tribunals
- The prevention of crime
- The investigation and detection of crime (including identification of offenders)
- Identification of witnesses
- To comply with a court order

8.2.2 Third parties must show lawful and adequate grounds for disclosure of footage. These may include but are not limited to:

- Police
- Statutory authorities with powers to prosecute, (e.g. H M Revenue and Customs, the Department for Work and Pensions, Trading Standards, etc.)
- Claimants in civil proceedings or solicitors acting for them
- Defendants in criminal proceedings or solicitors acting for them
- Other departments of the Council

8.2.3 Upon receipt from a third party of a valid request for the release of footage, the Council will exercise its discretion in accordance with its duties under the Data Protection Act 2018/ UK GDPR and:

- (i) Assess and process the request with reasonable speed; and
- (ii) Where it decides to comply with the request, ensure appropriate retention of footage which may be relevant to the request and make clear any time limit for retention.

## **9. REQUESTS FOR CCTV FOOTAGE BY MANCHESTER CITY COUNCIL STAFF FOR INTERNAL WORK-RELATED PURPOSES**

- 9.1 Every request by Council staff for the release of personal images generated by CCTV cameras for internal work-related purposes will be referred to the relevant CCTV Manager of his/her representative.
- 9.2 The member of staff submitting the request must demonstrate how it falls within the scope of the objectives set out in section 2 of this Code of Practice.
- 9.3 The member of staff submitting the request must also demonstrate that as far as reasonably practicable disclosure would be in accordance with the provisions of the UK General Data Protection Regulation, Data Protection Act 2018 and the Human Rights Act 1998.
- 9.4 Any member of staff who requires guidance as to whether their request for the release of CCTV footage for internal work-related purposes is lawful and reasonable should seek advice from the Democratic Services Legal Team.
- 9.5 The relevant CCTV Manager will determine whether it is appropriate to release the footage. Again if necessary advice should be sought from the Democratic Service Legal Team.
- 9.10 CCTV deployed by the Council for a planned covert purpose directed against a person where the surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware it is taking place **and** it is for a criminal law enforcement purpose which the Council has a power to investigate (which is punishable for a maximum term of at least 6 months in prison), may require a prior directed surveillance authorisation under RIPA 2000. Further guidance can be found in the Council's Corporate Regulation of Investigatory Powers Act (RIPA) and Investigatory Powers Act (IPA) policy which is available on the intranet. Staff **must** seek legal advice from the Democratic Service Legal Team on any proposed use of covert surveillance.

## **10 ASSESSMENT AND REVIEW**

### **10.1 Annual Review**

- 10.1.1 The operation of the CCTV cameras will be reviewed every year in accordance with the Surveillance Code's second guiding principle, to ensure the cameras' effectiveness and compliance with the Council's objectives. Any proposed changes or new risks identified will require the completion of a data protection impact assessment (DPIA) to consider whether the use of the CCTV cameras and any

proposed changes are necessary and proportionate in terms of their effects on people's privacy rights and comply with broader data protection obligations. Less intrusive methods that meet the same needs should be considered.

10.1.2 The annual review will also consider how use of the CCTV cameras complies with this Code, the ICO Code and the Surveillance Code.

10.1.3 Outside of the annual review, the Council may also draw up specific key objectives based on local concerns but if it wishes to extend the purposes for which the cameras are currently used it will not do so unless:

- (i) a data protection impact assessment has been completed
- (ii) relevant individuals and organisations who may be affected by the changes have been consulted; and
- (iii) the relevant DSIRO with responsibility for the CCTV cameras has approved the extended purposes in consultation with the Statutory Deputy Leader.

## **10.2 Changes to the Code**

10.2.1 This Code will be reviewed every two years unless there is a change in legislation or policy which warrants a review within that period.

10.2.2 Any major changes will require the approval of the Council's Executive on the recommendation of the Chief Officer with overall strategic responsibility for CCTV in consultation with the relevant Member of the Council's Executive who leads on CCTV.

10.2.3 Minor changes to this Code may be approved by the Chief Officer with overall strategic responsibility for CCTV.

## **10.3 Audit**

10.3.1 There will be regular audits of the operation of the CCTV cameras and compliance with this Code. Audits, which may be in the form of irregular spot checks, will include examining CCTV Control Room records and footage.

# **11. INFORMATION AND COMPLAINTS**

## **11.1 Information**

11.1.1 Requests for information may be made to the Infocompliance Group at:

Democratic Services Legal Team  
Legal Services  
PO Box 532

Town Hall  
Manchester  
M60 2LA  
Email: [informationcompliance@manchester.gov.uk](mailto:informationcompliance@manchester.gov.uk)

## **11.2 Complaints**

11.2.1 A member of the public wishing to register a complaint with regard to a data subject access request for footage, or in respect of another data subject right under data protection legislation, may do so by following the Council's [Information Rights Complaint Procedure](#) and by contacting the Council directly, such as by writing to the department that initially dealt with the request.

11.2.2 A member of the public wishing to register any other complaint with regard to the Council's use of CCTV cameras may do so by contacting the Council. All complaints will be dealt with in accordance with the Council's complaints procedure (as appropriate) and further information, including an online complaint form, can be obtained on the Council's website ([www.manchester.gov.uk](http://www.manchester.gov.uk)) or following this link [Manchester City Council](#).

11.2.3 Other methods of contacting the Council to submit a complaint are as follows;

By email – [complaints.feedback@manchester.gov.uk](mailto:complaints.feedback@manchester.gov.uk)

By phone – on 0161-234 5000

By textphone – this service is a means for hearing-impaired people to use the telephone as a method of contacting the Council. The number is 0161-234-3760.

By post – write to Customer Feedback, Corporate Performance Group, PO Box 532, Town Hall, Manchester M60 2LA

## **12. DISCIPLINARY ACTION AGAINST COUNCIL STAFF**

12.1 Breaches of this Code of Practice by Council staff will be dealt with in line with the Council's disciplinary procedure. Serious breaches could result in termination of the employment contract and where applicable may result in civil action and/or criminal charges.

## **Appendix 1 Data Protection Principles**

### **Article 5 UK GDPR Principles relating to processing of personal data**

1. Personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- (b) collected (whether from the data subject or otherwise) for specified, explicit and legitimate purposes and not further processed by or on behalf of a controller in a manner that is incompatible with the purposes for which the controller collected the data ('purpose limitation');
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 84B ('storage limitation');
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2.

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

3.

For the avoidance of doubt, processing is not lawful by virtue only of being processing in a manner that is compatible with the purposes for which the personal data was collected.

## **Appendix 2 Surveillance Code: Guiding Principles**

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then 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.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.



## Appendix 3 Template report



MANCHESTER  
CITY COUNCIL

### CCTV yearly report to Directorate Senior Information Risk Officer (‘DSIRO’)

[Specific CCTV system]

[Period covered]

#### 1. Introduction

1. Manchester City Council operates CCTV cameras within Manchester’s public areas and within and around its premises. The Council’s Code of Practice requires CCTV Managers to report to their relevant DSIRO on the operation of their CCTV system on a yearly basis. This is the report for the [insert specific CCTV system].

#### 2. Objectives of using CCTV cameras

2.1 The Council’s objectives in using CCTV cameras are:

- To assist in the deterrence and detection of crime (including environmental crime), disorder and anti-social behaviour in Manchester. This will include:
  - Countering terrorism
  - Helping to identify, apprehend and prosecute offenders
  - Providing evidence for criminal and civil action in the courts including preliminary investigation of claims
- To help reduce the fear of crime and provide reassurance to the public
- To increase safety for those people who live, work, trade within and visit Manchester including monitoring for security and safety purposes of Council staff and visitors on Council premises
- To assist in the overall management of public places

- To assist in developing the economic wellbeing of the Manchester area and encourage greater use of the City Centre
- To assist the Council in carrying out its regulatory functions in relation to environmental health and protection, pollution control, contaminated land, health and safety, food safety, animal welfare, consumer protection, weights and measures and licensing.
- To provide traffic management support and enforce bus lane and parking restrictions
- To provide assistance and direction in the event of a major emergency in Manchester

### 3. Performance

3.1 [The [insert specific CCTV system] has a Key Performance Indicator to reduce crime at an average of 10 locations which has been achieved during this period, see latest available results below.] Delete if not applicable

3.2 The tables below show the number of CCTV Generated Arrests, Data Subject Access requests, requests from GMP for copies of footage processed, FOI requests/general enquiries and complaints.

<b>CCTV generated arrests</b>	
Previous period	Current period

<b>Data subject access requests</b>	
Previous period	Current period

<b>Requests for copies of CCTV footage from GMP</b>	
Previous period	Current period

<b>FOI requests/general enquiries</b>	
Previous period	Current period

<b>Complaints</b>	
Previous period	Current period

**4. Maintenance and repair issues**

4.1 The table below shows the location and number of cameras requiring repair/replacement during the period.

<b>Repair/replacement</b>		
<b>Location</b>	<b>Number of cameras</b>	<b>Reason for repair/replacement (vandalism, fault, age, etc.)</b>

**5.0 Siting and operation**

5.1 Insert here whether siting and operation satisfactory or whether cameras are no longer necessary or should be relocated, changes in how they operate or how and where monitoring is carried out.

**6. Signage**

6.1 Insert here whether adequate signage is present to warn of operation of CCTV or any issues with signage, e.g. vandalism, complaints.

**7. Training**

7.1 Insert here staff training undertaken or needed and any training related issues.

**8. Any other relevant issues**

8.1 Insert here whether there are any other issues, e.g. problems about providing footage to third parties.

**9.0 DSIROs**

9.1 If you are unsure who your DSIRO is you can check via the following link:-

**[Information governance roles and responsibilities](#)**

Signed .....

Name.....

Position.....

Date.....