



MERTHYR TYDFIL
County Borough Council
Cyngor Bwrdeistref Sirol
MERTHYR TUDFUL

Merthyr Tydfil County Borough Council

CCTV Policy



<u>Issue Date</u>	<u>Version</u>	<u>History of Changes</u>	<u>Approval</u>
27/09/2017	1.0		Information Governance Forum
27/09/2018	1.0	No changes	Information Governance Forum (IGF)
18/10/2019	2.0	2.5 updated to include Weighbridge & Unit 20 Yard access 9.7 Removal of requirement of £10 fee for SAR Appendix 1 – PIA replaced with DPIA template	IGF
27/01/2021	2.0	Approved – no updates	IGF

Contents	Page No.
1. Introduction	4
2. Implementation Responsibilities	4
3. Objectives of CCTV Systems	4
4. Legislation	5
5. CCTV Operation	6
6. CCTV in Third-Party Occupied Buildings	6
7. Purchase and Deployment of CCTV Cameras	6
8. Covert Recordings	7
9. Access to CCTV Recordings	8
10. Retention	9
11. Breaches of this Policy	9
Appendix 1 – PIA Template	9
Appendix 2 – Request for ICT Evidence Form	9

1. Introduction

- 1.1 This Council uses Closed Circuit Television (CCTV) systems in public spaces, within car parks, at a number of owned sites across the county borough and within Council vehicles.
- 1.2 This policy along with the [ICO's CCTV Code of Practice](#) is designed to give clear guidelines on the Council's use of CCTV and to protect the Council and its CCTV operators from allegations of misuse of the system and to protect staff and the public from any abuse of the CCTV system.
- 1.3 This policy covers the use of CCTV equipment that has been installed by the ICT Department, and the gathering, storage, use and disposal of visual data. This policy applies to all staff employed at Merthyr Tydfil County Borough Council and should be the standard expected from any external agencies or persons who operate CCTV systems on its behalf. No CCTV cameras should be installed independently, **all requests for CCTV must be made via the ICT Department.**

2. Implementation Responsibilities

- 2.1 The Information Security Officer shall develop, maintain, and publish processes to achieve compliance with this policy. Any queries regarding this policy can be directed to 01685 727444 or via email, information.security@merthyr.gov.uk
- 2.2 All Managers will be responsible for implementing this policy within their areas of responsibility. All employees, Members and third-parties shall sign the Information Security Policy to indicate their agreement to comply with the CCTV Policy.
- 2.3 The Council takes seriously its statutory responsibilities and will, always, act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard, the Information Governance Forum is duly authorised by the Council to keep this Policy up to date and to amend, delete, add or substitute relevant provisions, as necessary, in consultation with the Cabinet Member for Governance and Corporate Services
- 2.4 The day-to-day operational responsibility rests with the designated staff within the ICT Department who operate the CCTV equipment and handle the data.
- 2.5 Within Environmental Services, a restricted number of staff operate the CCTV equipment that is recording within Council vehicles, used for the Weighbridge System, and for Health & Safety purposes within the Unit 20 Yard.

3. Objectives of CCTV Systems

- 3.1 It is important that everyone and especially those charged with operating the CCTV systems on behalf of Merthyr Tydfil County Borough Council understand exactly why each of the systems has been introduced and what the cameras will and will not be used for.

3.2 Each CCTV system will have its own site or task specific objectives. These will include some or all of the following:

- **Protecting areas and premises used by council staff and the public;**
- **Deterring and detecting crime and anti-social behaviour;**
- **Assisting in the identification of offenders leading to their arrest and successful prosecution or other appropriate action;**
- **Reducing violent or aggressive behaviour towards staff;**
- **Reducing fear of crime, anti-social behaviour and aggression;**
- **Protecting Council property and assets;**
- **Assisting in staff disciplinary, grievance, formal complaints and Health and Safety investigations.**

3.3 The systems will not be used for any other purpose than those set out in this policy without prior consultation with the Council's Senior Information Risk Owner (SIRO), and where appropriate, notification to staff, Members and third-parties, following consultation with the Trade Unions. Any novel or non-standard use of the CCTV cameras are to require the approval of the SIRO.

3.4 Cameras will not be used to monitor the progress of staff or individuals in the ordinary course of lawful business in the area under surveillance. Nor are managers permitted to use the cameras to observe staff working practices or to assist them in the day to day management of their staff.

3.5 Individuals will only be monitored if there is reasonable cause to suspect a criminal offence or serious breach of discipline, potentially amounting to misconduct has been, or may be, about to be committed and this will only be permitted when authorised and may require the use of RIPA authorisation. Managers will need to complete an 'ICT Evidence Request' form (available in Appendix 2) for access to CCTV footage.

4. Legislation

4.1 In addition to Council policies, procedures, guidelines and Codes of Practice, CCTV and its operation are subject to legislation under:

- Data Protection Law
- The Human Rights Act 1998 (HRA)
- The Freedom of Information Act 2000 (FOIA)
- The Regulation of Investigatory Powers Act 2000 (RIPA)
- The Protection of Freedoms Act 2012

4.2 Where images of living, identifiable individuals are recorded, this is likely to compromise those individual's personal data. The collection use and storage of personal data are governed by Data Protection Law. MTCBC is a data controller registered with the Information Commissioners Office (ICO).

- 4.3 Given that any particular sequence of CCTV recording may include personal data; all such recordings will be processed in accordance with Data Protection Law.
- 4.4 Where a data subject requests access to their personal data, you should refer to section 9 of this policy.
- 4.5 It is important that the operation of all Council installed CCTV systems comply with these Acts, policies, procedures, guidelines and Codes of Practice, to ensure that the Council, staff operating the CCTV systems and the public are protected from abuses of the CCTV systems.

5 CCTV Operation

- 5.1 The ICT Operations Manager is responsible for the day-to-day management of the CCTV system and making sure authorised staff (the Information Security Officer, the ICT Infrastructure Team, any other person authorised to view images) using the CCTV system are properly trained in the use of equipment and comply with the Code of Practice and this policy. No other staff member is permitted to operate the equipment without authorisation from the ICT Operations Manager.
- 5.2 The Team Leader – Environmental Services, is responsible for the day-to-day management of the CCTV systems installed within refuse vehicles and the Unit 20 Yard, and making sure authorised staff using the CCTV system are properly trained in the use of this equipment and comply with the Code of Practice and this policy.
- 5.3 The Information Security Officer will act as the first point of contact for enquiries, complaints and requests for evidence.
- 5.4 Staff operating CCTV systems are responsible for operating the equipment in accordance with requirements set out in current legislation, this policy document, Codes of Practice and local operation manuals.
- 5.5 Staff operating CCTV systems are responsible for bringing any faults or misuse of the equipment to the Information Security Officer's attention immediately.

6 CCTV in Third Party Occupied Buildings

- 6.1 A number of Council owned CCTV systems may be located in premises other than those occupied by the Council. In these instances, it is important that there is a clear understanding between the Council and the people in the properties concerned as to what these CCTV systems may be used for and who is responsible for each aspect of the system. Responsible Officers within the third party occupied building will be required to complete an ICT Request Form and Data Protection Impact Assessment (DPIA).

7 Purchase and Deployment of CCTV Cameras

- 7.1 MTCBC is committed to respecting people's rights to privacy and supports the individual's entitlement to go about their lawful business. This is a primary consideration in the operation of any CCTV system, although there will inevitably be some loss of privacy when CCTV cameras are installed.
- 7.2 It is crucial that serious consideration is given to the necessity for cameras in a given location, and their impact on the privacy of individuals.
- 7.3 Cameras are not to be installed in such a way that they can look into private spaces.
- 7.4 Conversations between staff, Members, third-parties and members of the public must not be recorded on CCTV.
- 7.5 MTCBC will not use CCTV cameras if there are cheaper, less intrusive and more effective methods of dealing with the problem.
- 7.6 If after looking at all the alternatives it is decided that CCTV is the only suitable solution and there is a clear operational objective for the system, an assessment on the impact on privacy must be carried out (see Appendix 1).
- 7.7 Once a decision has been made to purchase CCTV cameras, advice should be sought from the Council's ICT Department. CCTV cameras and systems MUST only be purchased via the ICT Department to ensure that the correct procedures are followed. Requests for CCTV must be submitted to ICT via a 'Request for ICT Services' form.
- 7.8 The Council's Printing & Design Team will produce appropriate signage which must be placed in areas where CCTV is deployed.

8 Covert Recording

- 8.1 Covert cameras are not normally to be deployed into areas used by staff, Members, third-parties or the public. Cameras should normally be clearly visible and clearly signed.
- 8.2 Covert cameras may be used within pre-defined CCTV areas under the following circumstances on the written authorisation of the SIRO and where a DPIA has been completed:
 - That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
 - That there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.
- 8.3 Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity.
- 8.4 The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

8.5 Staff, Members and third-parties working on behalf of the Council must not set up their own cameras for recording purposes within Council buildings, Council vehicles, or third-party owned buildings that the Council occupies.

8.6 Staff, Members and third-parties working on behalf of the Council must not record footage or audio on mobile devices within Council buildings, Council vehicles, or third-party owned buildings that the Council occupies.

9 Access to CCTV Recordings

9.1 Images captured by the CCTV system will be monitored within the ICT Department, where only designated staff, have access to enter the department.

9.2 For operational purposes and in accordance with the stated purposes of the system, only designated staff shall have primary access to CCTV recordings.

9.3 The ICT Operations Manager or Information Security Officer may permit the viewing of CCTV recorded materials by Police and other staff where this is necessary in connection with a serious occurrence. They will have authority for making a decision regarding who should have access to this data other than designated staff and ensuring that data is used appropriately.

9.4 Pre-recorded CCTV data should not be downloaded due to potential breach of Data Protection Law. Data should only be downloaded or saved if it forms part of an investigation into a serious occurrence including staff conduct or Police matter.

9.5 Requests for data should come from Human Resources & Development, Audit, the Data Protection Officer following a Subject Access Request, or the Police only.

9.6 Requests for data should be made via an 'ICT Evidence Request Form' (Appendix 2) and submitted to the Information Security Officer.

9.7 Data Subjects may make a [Subject Access Request](#) for CCTV images/recordings by applying in writing to Legal Services and must provide the following information:

- Dates and times of the incident or their visit to a building (specific location must be provided) where MTCBC has internal CCTV cameras installed
- A photograph to enable the CCTV operators to identify them in the recorded footage
- Proof of identity

A response will be provided within one calendar month.

9.8 MTCBC has the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

- 9.9 If it is decided that a subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

10 Retention

- 10.1 CCTV recordings and other materials produced from them shall be retained for a period of three months unless an incident is recorded which requires further investigation. In the latter case, recordings shall be kept for a period of three years from the date of recording.
- 10.2 All media no longer required, on which recordings were made will be returned to the ICT Department for destruction.

11 Breaches of this Policy

- 11.1 Breaches of this policy should be reported immediately, but no later than 72 hours after the incident, to the Information Security Officer. For details on how to report an incident, please refer to the Council's 'Reporting Information Security Incidents Policy' on the Intranet.
- 11.2 Breaches of this Policy will be considered under the Council's Disciplinary Policy.

Appendix 1 – Privacy Impact Assessment



Data Protection
Impact Assessment.x

Appendix 2 – ICT Evidence Request Form



ICT Evidence
Request Form.doc
