



DEPARTMENT OF JUSTICE, EQUALITY AND LAW REFORM  
AN ROINN DLÍ AGUS CIRT, COMHIONANNAIS AGUS ATHCHÓIRITHE DLÍ

# **CODE OF PRACTICE FOR COMMUNITY- BASED CCTV SYSTEMS**

## **INTRODUCTION**

This Code of Practice sets out the basic conditions of use for Community-Based CCTV systems by applicants for the Department of Justice, Equality and Law Reform's grant-aid scheme.

All persons involved in the planning, supervision or operation of such a CCTV scheme should familiarise themselves with this document from the outset.

It is of crucial importance in order to maintain public confidence in the operation of Community-Based CCTV systems that there is no improper use of the equipment. Any misuse of CCTV systems is likely to damage the positive perception of CCTV in the eyes of the public. Compliance with this Code of Practice governing Community-Based CCTV systems and their operation will not only assist CCTV scheme operators to act in accordance with law but also aid in maintaining the confidence of the public in the systems.

This Code of Practice is designed to assist operators of CCTV systems by highlighting certain legal obligations set down in the Data Protection Acts, 1988 and 2003. In order for this Code of Practice to remain relevant to the day to day activities of CCTV operation, it needs to be constantly updated as practice and understanding of the laws in this area develop. Accordingly, this Code will be kept under review to ensure that it remains relevant in the context of changes in technology, and compliant with any developments in this area.

## **(1) Initiation of a CCTV System**

- (1.1) The purposes of any CCTV system qualifying for grant aid under this scheme should include:
- assistance in the maintenance of public order and safety;
  - assistance in the prevention, detection and investigation of offences;
  - assistance in the prosecution of offenders.
- (1.2) Only persons authorised by the Community-Based Group shall be permitted access to the control area where monitoring takes place.
- (1.3) The Community-Based Group will at all times ensure the proper and responsible operation of the CCTV system under their control and ensure that all persons operating or monitoring the system are appropriately trained in the system's use and understand the restrictions and legal obligations imposed upon them by the laws in this area. For the purposes of the Data Protection Act, 1988, each Local Authority must undertake to act as the Data Controller.
- (1.4) It is the responsibility of the Community-Based Group to ensure that all uses of the system are appropriate and in the interest of the community.
- (1.5) A manager or designated person should be nominated by the Data Controller. This individual will have responsibility for ensuring the proper, efficient and orderly day to day operation of the CCTV system.
- (1.6) The Community-Based Group shall maintain an appropriate record of the system's effectiveness.
- (1.7) Respect for the individual's liberty and privacy where no criminal offence has been or is being committed should be of primary consideration.

## **(2) Siting Standards**

- (2.1) Cameras should be sited in such a way that they only monitor those spaces which are intended to be covered by the system.
- (2.2) Operators must be aware of the purposes for which the scheme has been established.
- (2.3) Operators must be aware that they may only use the cameras in order to achieve the purposes for which the system has been installed. Care must be taken not to use the cameras to look into any premises, be they public houses, shops, business premises or private dwellings. This approach must likewise be taken with any demonstration of the capabilities of the cameras.
- (2.4) Operators must also be aware of the position a camera is left in after use. A camera when not in use should be placed in the most advantageous position to record any incidents occurring in a public area within its field of vision.
- (2.5) Signs should be placed so that the public are aware that they are entering an area which is covered by a CCTV system. These signs should be clearly visible and legible to members of the public. Such signs should contain the following information:
  - (a) the identity of the person or organisation responsible for the CCTV scheme.
  - (b) the purposes of the scheme.
  - (c) details of who to contact regarding the scheme.

### **(3) Quality of the Images**

- (3.1) Upon installation an initial check should be undertaken to ensure that all equipment performs properly.
- (3.2) If tapes are used, it should be ensured that they are good quality tapes.
- (3.3) The medium on which the images are captured should be regularly cleaned so that images are not recorded on top of images recorded previously.
- (3.4) The medium on which the images have been recorded should not be used when it has become apparent that the quality of images has deteriorated.
- (3.5) If the system records features such as the location of the camera and/or date and time reference, these should be accurate.
- (3.6) If the system includes location and date/time reference features, users should ensure that they have a documented procedure for ensuring their accuracy.
- (3.7) Cameras should be situated so that they will capture images relevant to the purpose for which the scheme has been established.
- (3.8) When installing cameras, consideration must be given to the physical conditions in which the cameras are located.
- (3.9) Users should assess whether it is necessary to carry out constant real time recording, or whether the activity or activities about which they are concerned occur at specific times.
- (3.10) Cameras should be properly maintained and serviced to ensure that clear images are recorded.
- (3.11) Cameras should be protected from vandalism in order to ensure that they remain in working order.
- (3.12) A maintenance log should be kept by the Data Controller.
- (3.13) If a camera is damaged, there should be clear procedures for:
  - (a) defining the person responsible for making arrangements for ensuring that the camera is repaired.
  - (b) ensuring that the camera is repaired within a specific time period.
  - (c) monitoring the quality of the maintenance work.

#### **(4) Processing of CCTV Images**

(4.1) All tapes will be stored in lockfast facilities to which access is restricted within the CCTV control area at all times except when:-

- (i) They are requested by the Garda authorities and such a request being authorised by a member of at least the rank of Inspector.
- (ii) They are requested through the judicial process.

Tapes held should be counted daily and a record kept by the Data Controller or designated person acting on the Data Controller's behalf.

(4.2) Images should not be retained by the Data Controller for longer than is necessary. Images will be erased and tapes re-used after a period of 31 days unless required for the investigation of offences or evidential purposes.

(4.3) Only persons authorised by the Data Controller shall be allowed access to the tapes used in the CCTV system.

(4.4) Access to the recorded images should be restricted by the Data Controller to a designated person or persons. Other persons should not be allowed to have access to that area when a viewing is taking place.

(4.5) Copies of tapes are not to be made by the Community-Based Group. If copies are to be made, the Data Controller will do so in any of the following circumstances:

- i. the incident recorded is of a serious nature (eg. one that may lead to criminal proceedings).
- ii. a formal request from a member of An Garda Síochána (of at least the rank of Inspector),
- iii. the incident recorded is proceeding to trial.
- iv. a request to view the tape is received from the DPP.
- v. the circumstances are such that repeated playing of the incident recorded on tape is required (i.e. to show to witnesses).
- vi. where a copy is required in order to satisfy a subject access request.

(4.6) In the circumstances set out at Section 4.5, the original tape will be retained by the Data Controller until it is necessary to take it to Court. An original tape shall remain in the possession of the Data Controller or a person designated to act on its behalf unless the original is required:

- (i) for the purpose of court proceedings;
- (ii) by or under any other enactment.

- (4.7) On removing the medium on which the images have been recorded, the Data Controller should ensure that they have documented:
- (a) the date on which the images were removed from the general system;
  - (b) the reason why they were removed from the system;
  - (c) any crime incident number to which the images may be relevant;
  - (d) the location of the images;
  - (e) the signature of the collecting official, where appropriate.
- (4.8) Removal of the medium on which images are recorded, for viewing purposes, should be documented as follows:
- (a) the date and time of the removal.
  - (b) the name of the person removing the images.
  - (c) the name(s) of the person(s) viewing the images. (If this should include third parties, the name of the organisation to which the third party belongs).
  - (d) the reason for the viewing.
  - (e) the outcome, if any, of the viewing.
  - (f) the date and time the images were returned to the system or secure place, if they have been retained for evidential purposes.
- (4.9) All operators and employees with access to images should be made aware by the Data Controller of the procedures which need to be followed when accessing the recorded images.
- (4.10) It is the responsibility of the Data Controller to ensure that all operators are trained in their responsibilities under this Code of Practice (i.e. they should be aware of :
- (a) the user's security policy (*eg. procedures for access to recorded images*).
  - (b) the user's disclosure policy.
- (4.11) The use of automatic facial recognition technologies is prohibited, pending any future revision of this Code in the light of data protection requirements.

## **(5) Access to and Disclosure of Images to Third Parties**

- (5.1) Access to images should be restricted to those staff who need to have access in order to achieve the purposes of using the equipment.
- (5.2) All access to the medium on which the images are recorded should be documented by the Data Controller or a manager or designated member of staff acting on the Data Controller's behalf.
- (5.3) Disclosure of the recorded images to third parties should only be made by the Data Controller in limited and prescribed circumstances. Circumstances in which disclosure is appropriate would, for example, include
  - (a) a formal request from a member of An Garda Síochána (of at least the rank of Inspector), for disclosure of images, on the grounds that the images are likely to be of use for the investigation of a particular offence;
  - (b) a requirement under any enactment, rule of law or court order to disclose the images;
  - (c) if required by the Data Controller's legal representatives if a case/action is being taken against the Community-Based Group;
  - (d) the media, where it is decided 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 decision, the wishes of the victim of an incident should be taken into account. The release of images to the media in a criminal investigation is solely within the remit of An Garda Síochána.
  - (e) people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal inquiries or criminal proceedings).
- (5.4) All requests for access for disclosure should be recorded by the Data Controller. If access or disclosure is denied, the reason should be documented.
- (5.5) If access to or disclosure of the images is allowed, then the following should be documented:
  - (a) the date and time at which access was allowed or the date on which disclosure was made;
  - (b) the identification of any third party who was allowed access or to whom disclosure was made;
  - (c) the reason for allowing access or disclosure;
  - (d) the extent of the information to which access was allowed or which was disclosed;
  - (e) the identity of the officer authorising such access.



- (5.6) Where the images are determined to be personal data, if it is decided that images will be disclosed to the media, the images of individuals may need to be disguised or blurred so that they are not readily identifiable.
- (5.7) If the system does not have the facilities to carry out that type of editing, an editing company may need to be hired to carry it out.
- (5.8) If an editing company is hired, then the manager or designated member of staff needs to ensure that:
- (a) there is a contractual relationship between the Data Controller and the editing company;
  - (b) that the editing company has given appropriate guarantees regarding the security measures they take in relation to the images;
  - (c) the Data Controller shall have in place appropriate and adequate procedures to ensure those guarantees are met including a right of access to the contractor's premises or systems;
  - (d) the written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the Data Controller or a manager or designated member of staff acting on the Data Controller's behalf;
  - (e) the written contract makes the security guarantees provided by the editing company explicit.
- (5.9) If a media organisation as referred to at Section 5.3(d) receiving the images undertakes to carry out the editing, then (a) to (e) above will still apply.

## **6. Access by Data Subjects**

### **Data Subject Access Standards**

- (6.1) All staff involved in operating the equipment must be able to recognise a request by data subjects for access to personal data in the form of recorded images by data subjects.
- (6.2) Data subjects may be provided with a standard subject access request form which:
  - (a) indicates the information required in order to locate the images requested;
  - (b) indicate that a fee will be charged for carrying out the search for the images requested. The maximum fee which may be charged for the supply of copies of data in response to a subject access request is set out in the Data Protection Acts, 1988 and 2003;
  - (c) ask whether the individual would be satisfied with merely viewing the images recorded;
  - (d) indicate that the response will be provided promptly following receipt of the required fee and in any event within 40 days of receiving adequate information.
- (6.3) Staff operating the system should be able to explain to members of the public the type of images which are recorded and retained, the purposes for which those images are recorded and retained, and information about the Group's disclosure policy in relation to those images. Staff may find it valuable to have a leaflet available as an aid to any such explanation.
- (6.4) If available, this leaflet should be provided at the time that the standard subject access request form is provided to an individual.
- (6.5) All data subject access requests should be dealt with by a manager or designated member of staff whose identity is known to other staff members (See paragraph 1.5).
- (6.6) The manager or designated member of staff should locate the images requested.
- (6.7) The manager or designated member of staff should determine whether disclosure to the individual would entail disclosing images of third parties.
- (6.8) If third party images are not to be disclosed, as in Section 6.7, the manager or designated member of staff shall arrange for the third party images to be disguised or blurred.
- (6.9) If the system does not have the facilities to carry out the type of editing required at (6.8) above, a third party or company may be hired to carry it out.
- (6.10) If a third party or company is hired, then the manager or designated member of staff needs to ensure that:

- (a) there is a contractual relationship between the Data Controller and the third party or company;
  - (b) that the third party or company has given appropriate guarantees regarding the security measures they take in relation to the images;
  - (c) The Data Controller shall have in place appropriate and adequate procedures to ensure those guarantees are met including a right of access to the contractor's premises or systems;
  - (d) The written contract makes it explicit that the third party or company can only use the images in accordance with the instructions of the manager or designated member of staff.;
  - (e) The written contract makes the security guarantees provided by the third party or company explicit.
- (6.11) It is the responsibility of the Data Controller to ensure that all staff are aware of an individual's rights under relevant Data Protection Legislation as well as those mentioned under this Code of Practice.

## **7. Miscellaneous Data Subject Rights**

- (7.1) All staff involved in operating the CCTV equipment must be able to recognise a request from an individual to:
  - (a) rectify or erase, where appropriate, personal data.
  - (b) prevent processing likely to cause substantial and unwarranted damage to that individual, unless a legitimate reason exists for such processing.
  - (c) prevent automated decision taking (ie. automatic facial recognition) in relation to that individual.
- (7.2) All staff must be aware of the identity of the manager or designated member of staff who is responsible for responding to such requests.
- (7.3) In relation to a request for rectification, erasure or to prevent processing likely to cause substantial and unwarranted damage, the manager or designated member of staff's response should indicate whether he or she will comply with the request or not.
- (7.4) The manager 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.
- (7.5) If the manager or designated member of staff decides that the request will not be complied with, they must set out their reasons in their response to the individual.
- (7.6) A copy of the request and response should be retained and filed securely.
- (7.7) The manager or designated member of staff shall document:
  - (a) the request from the individual;
  - (b) the original decision;
  - (c) their response to the request from the individual;
  - (d) the reasons for rejection, if applicable.

## **8. Monitoring Compliance with this Code of Practice**

It is the responsibility of the Data Controller to ensure that there is full compliance with this Code of Practice. Contravention of a provision of the Data Protection Acts 1988 and 2003 may expose a person to prosecution under the Act.

### **Monitoring Standards**

- (8.1) The contact point indicated on the sign should be available to members of the public during office hours. Employees staffing that contact point should be aware of the policies and procedures governing the use of the Community-Based Group's CCTV equipment.
- (8.2) Enquirers should be provided on request with one or more of the following:
  - (a) the leaflet, if available, for the purpose of general information which enquirers may receive when they make a subject access request;
  - (b) a copy of this Code of Practice;
  - (c) a data subject access request form if required or requested;
  - (d) the complaints procedure to be followed if an enquirer has concerns about the use of the system;
  - (e) the complaints procedure to be followed if an enquirer has concerns about non-compliance with the provisions of this Code of Practice;
  - (f) no fee may be charged in respect of the provision of any of the above documents.
- (8.3) A complaints procedure should be clearly documented by the Data Controller.
- (8.4) A record of the number and nature of complaints or enquiries received should be maintained by the Data Controller together with an outline of each action taken.
- (8.5) A report on those numbers should be collected by the manager or designated member of staff in order to assess public reaction to, and opinion of, the use of the system.
- (8.6) A manager or designated member of staff should undertake regular reviews of the documented procedures to ensure that the provisions of this Code of Practice are being complied with. Such an audit should be carried out on at least an annual basis.
- (8.7) A report on those reviews should be provided to the Data Controller in order that compliance with legal obligations and provisions of this Code of Practice can be monitored.
- (8.8) An internal annual assessment should be undertaken which evaluates the effectiveness of the system. The audit referred to at (8.6) may form part of such an assessment.
- (8.9) The results of the report should be assessed against the stated purpose of the scheme. If the scheme is not achieving its purpose, it should be reviewed or modified where necessary.