An Roinn Dlí agus Cirt
Department of Justice

DEPARTMENT OF JUSTICE

AN ROINN DLÍ AGUS CIRT

AN GARDA SÍOCHÁNA

CODE OF PRACTICE FOR COMMUNITY BASED CCTV SYSTEMS

Introduction

This Code of Practice sets out the conditions applicable to community based CCTV systems.

Section 38 of the Garda Síochána Act, 2005 lays down the conditions governing the operation of CCTV schemes in a public place. This includes the need for all CCTV schemes operating in public areas to have written authorisation of the Garda Commissioner. Section 38(1) provides as follows:

> "*The Garda Commissioner may authorise the installation and operation of CCTV for the sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences."*

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 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. 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.

Definition

For the purposes of this document, "media storage device" means any device, including CDs, DVDs cassette tapes, USB sticks, hard drives etc., which is capable of storing digital or analogue information.

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 (in this document referred to as the operator) operating the system can be permitted access to the control area where monitoring takes place.

1.3 The operator 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 by the system installer or other qualified persons. Owners and operators should also understand the restrictions and legal obligations imposed upon them by the laws in this area with

particular reference to criteria laid down in Section 38 of the Garda Síochána Act 2005 and the Garda Síochána (CCTV) Order 2006 (S.I. No. 289 of 2006).

1.4 For the purposes of the Data Protection Act, 1988 and 2003 and the Garda Síochána (CCTV) Order 2006 (S.I. No. 289 of 2006), each Local Authority must undertake to act as the Data Controller.

1.5 It is the responsibility of the operator to ensure that all uses of the system are appropriate and in the interest of the community.

1.6 An official 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. A condition of the CCTV application and referred to in the Application Guidelines Document (Form No – PD002) is that Garda vetting must be carried out in respect of the proposed data controller and others who will have access to the system.

1.7 The operator must maintain an appropriate record of the system's effectiveness. – see paragraph 8.8.

1.8 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 and Signage

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 On occasions when not being actively monitored by an operator, all operating cameras 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 CCTV Images

3.1 Upon installation, an initial check should be undertaken to ensure that all equipment performs properly.

3.2 If media storage devices are being used, they should be of a high quality.

3.3 The equipment being used to capture image material should be maintained to a level where the quality of the images from the equipment meet the standard required by the Garda Technical Specification document.

3.4 The media storage devices onto which the images have been recorded should not be used when it has become apparent that they can no longer be used to store images of the quality required.

3.5 If the system records details such as the location of the camera and/or the date and time reference, these should be accurate and users should ensure that they have a documented procedure for ensuring their accuracy.

3.6 Cameras should be situated so that they will capture images relevant to the purpose for which the scheme has been established.

3.7 When installing cameras, consideration must be given to the physical conditions in which the cameras are located. The security of the camera should also be taken into consideration when deciding on its location.

3.8 Cameras should be properly maintained and serviced to ensure that clear CCTV images are recorded.

3.9 Cameras should be protected from vandalism in order to ensure that they remain in working order.

3.10 Operators 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.

3.11 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.

3.12 A maintenance log should be kept by the Data Controller.

4. Processing of CCTV Images

4.1 All removable/portable media storage devices should be stored in secure facilities to which access is restricted within the CCTV control area at all times except when:

(a) they are requested by the Garda authorities and such a request is authorised by a member not below the rank of Superintendent or

(b) they are requested through the judicial process.

Portable/removable media storage devices 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 CCTV images should not be retained by the Data Controller for longer than is necessary. The Data Protection Commissioner's guidance is that CCTV images should be retained for no more than 28 days unless there are specific, legitimate and

reasonable grounds for the retention of images beyond that period. CCTV images should be erased and media storage devices re-used after a period of 28 days unless required for the investigation of offences or evidential purposes. Media storage devices which cannot be erased (e.g. single use CD/DVDs) should be destroyed after a period of 28 days unless required for the investigation of offences or evidential purposes.

4.3 Only persons authorised by the Data Controller can be allowed access to the media storage devices used in the CCTV system.

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

4.5 Copies of media storage devices are not to be made by the operator. If copies are to be made, the Data Controller will do so in any of the following circumstances:

(a) the incident recorded is of a serious nature (e.g. one that may lead to criminal proceedings);

(b) following a formal request from a member of An Garda Síochána not below the rank of Superintendent;

(c) the incident recorded is proceeding to trial;

(d) a request to view the media storage device is received from the DPP;

(e) the circumstances are such that repeated playing of the incident recorded on a media storage device is required (i.e. to show to witnesses); or

(f) where a copy is required in order to satisfy a subject access request.

4.6 In the circumstances set out at Paragraph 4.5, the original media storage device will be retained by the Data Controller until it is necessary to take it to Court. An original media storage device must remain in the possession of the Data Controller or a person designated to act on his or her behalf unless the original is required:

(a) for the purpose of court proceedings or

(b) by or under any other enactment.

4.7 On removing the media storage device on which the CCTV images have been recorded, the Data Controller should ensure that he or she has documented:

(a) the date on which the media storage device was removed from the system;

(b) the reason why it was removed from the system;

(c) any crime incident number to which the media storage device may be relevant;

(d) the location of the media storage device; and

(e) the signature of the collecting official, where appropriate.

4.8 The following details should be recorded when a media storage device on which media is stored is removed for viewing purposes:

(a) the date and time of the removal;

(b) the name of the person removing the media storage device;

(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; and

(f) the date and time the media storage device was returned to the system or secure place, if it has been retained for evidential purposes.

4.9 It is the responsibility of the Data Controller to ensure that all operators are trained in their responsibilities under this Code of Practice and in particular they should be aware of:

(a) the operator's security policy (e.g. procedures for access to recorded CCTV images); and

(b) the operator's disclosure policy.

4.10 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 CCTV Images to Third Parties

5.1 Access to CCTV images should be restricted to those staff who need to have access in order to achieve the purposes of the CCTV system.

5.2 All access to media storage devices onto which 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 CCTV images to third parties should only be made by the Data Controller in limited circumstances including:

(a) following a formal request from a member of An Garda Síochána not below the rank of Superintendent 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 where legal proceedings are being taken against the operator;

(d) media organisations, 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. ***Note: The release of CCTV images to the media in a criminal investigation is solely within the remit of a member of An Garda Síochána not below the rank of Superintendent;*** or

(e) to 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 reasons 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 Data Controller 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 in writing 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 must 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; and

(e) the written contract makes the security guarantees provided by the editing company explicit.

5.9 If a media organisation as referred to at Paragraph 5.3(d) receiving the images undertakes to carry out the editing, then Paragraph 5(8)(a) to (e) will apply to the media organisation as if that organisation were the editing company referred to in Paragraph 5.

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 that has been captured by the system.

6.2 Data subjects should be provided with a standard access request form which:

(a) enables the data subject to indicate the information required in order to locate the images requested;

(b) may 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) enables the data subject to indicate whether his or her request for access to the data would be satisfied by viewing the images recorded; and

(d) specifies 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 operator'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 all staff members (See paragraph 1.6).

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 the manager or designated member of staff must 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 Paragraph 6.8 a suitable editing company may be hired to carry it out.

6.10 If a suitable editing company is hired, then the manager or designated member of staff needs to ensure that the provisions of Paragraphs 5.8(a) to 5.8(e) are complied with.

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; or

(c) prevent automated decision taking (i.e. automatic facial recognition) in relation to that individual.

7.2 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 or not he or she will comply with the request.

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

7.4 If the manager or designated member of staff decides that the request will not be complied with, he or she must set out the reasons in the response to the individual.

7.5 A copy of the request and response should be retained and filed securely.

7.6 The manager or designated member of staff must document:

(a) the request from the individual;

(b) the original decision;

(c) the response to the request from the individual; and

(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 those Acts.

Monitoring Standards

8.1 The contact point indicated on the sign (see Paragraph 2.5) should be available to members of the public during office hours. Employees who are staffing that contact point should be aware of the policies and procedures governing the use of the operator's CCTV equipment.

8.2 Persons making enquiries should be provided on request and free of charge with one or more of the following:

(a) the leaflet, if available, referred to at Paragraph 6.3;

(b) a copy of this Code of Practice;

(c) a standard access request form if required or requested (see Paragraph 6.2)

(d) information in relation to the complaints procedure to be followed where the person has concerns about the use of the system or non-compliance with this Code of Practice, as the case may be.

8.3 Complaints procedures 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 action taken in respect of each complaint or enquiry.

8.5 A report on the nature of complaints referred to in paragraph 8.4 should be prepared 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 (at least annually) of the documented procedures to ensure that the provisions of this Code of Practice are being complied with.

8.7 A report on each review referred to in paragraph 8.6 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 must be undertaken which evaluates the effectiveness of the system. The review referred to at Paragraph 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.