



# CCTV Policy

2017

Approved by the Board Of Management.  
15<sup>th</sup> May 2017

---

# Nenagh Community Training Centre (NCTC)

## INTRODUCTION

Closed Circuit Television Systems (CCTVS) are installed in Nenagh Community Training Centre (NCTC) and have been introduced in consultation with staff and the board of management.

### 1. PURPOSE OF POLICY

“This policy aims to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of NCTC.”

### 2. OBJECTIVES

CCTV systems are installed (internally and externally) around the premises for the purpose of assisting in providing a safe and secure environment for the benefit of those who might visit or work therein. Specifically, CCTV surveillance at NCTC is intended for the purposes of:

- Promoting the health and safety of staff, learners and visitors.
- Protecting NCTC buildings and assets, both during and after hours of business.
- Preventing bullying.
- Reducing the incidence of crime and anti-social behaviour (including theft and vandalism).
- Supporting the Gardaí in a bid to deter and detect crime (i.e. assisting in identifying, apprehending and prosecuting offenders).
- Assisting in conflict resolution where necessary.
- Ensuring that NCTC rules are respected so that the Centre can be properly managed.

### 3. SCOPE

This policy relates directly on the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. Where classes and activities are carried

out in rented premises, NCTC will ensure that CCTV systems, where installed, are operated only in a way that is compatible with the provisions of this policy.

#### **4. GENERAL PRINCIPLES**

NCTC as the corporate body has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, learners and invitees to its premises. NCTC owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for enhancing the quality of life of NCTC by integrating the best practices governing the public and private surveillance of its premises.

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

Information obtained through the CCTV system may only be released when authorised by the Manager (who for the purposes of this policy is the nominated Data Controller for the CCTV System) following consultation with the Chairperson of the Board of Management. Any requests for CCTV recordings/images from An Garda Síochána will be fully recorded and legal advice will be sought if any such request is made (See “Access” below). If a law enforcement authority, such as An Garda Síochána is seeking a recording for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request made by An Garda Síochána should be requested in writing and NCTC will immediately seek legal advice.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by NCTC, including Equality & Diversity Policy, Dignity at Work Policy, Data Protection Policy, Codes of Practice for dealing with complaints of Bullying &

Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and other educational related legislation.

This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

Video monitoring of public areas for security purposes within NCTC premises is limited to uses that do not violate the individual's reasonable expectations to privacy.

All CCTV systems associated equipment will be required to be compliant with this policy following its adoption by NCTC. Recognisable images captured by CCTV systems are "personal data". There are therefore subject to the provisions of the Data Protection Acts 1988 and 2003.

## 5. JUSTIFICATION FOR USE OF CCTV

Section 2(1) (c) (iii) of the Data Protection Acts requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that NCTC needs to be able to justify the obtaining and use of personal data by means of a CCTV system.

*The Board of Management has authorised the use of CCTV in accordance with this Policy.*

***CCTV systems will not be used to monitor normal instructor/learner classroom activity in the centre.***

## 6. LOCATION OF CAMERAS

The location of cameras is a key consideration. NCTC has endeavoured to select locations for the installation of CCTV cameras that are the least intrusive to the privacy of individuals. Cameras placed to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

**CCTV Video Monitoring and Recording of Public Areas in NCTC include the:**

- **Protection of buildings and property:** the building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services.
- **Monitoring of Access Control Systems:** monitor and record restricted access areas at entrances to buildings and other areas.
- **Verification of Security Alarms:** intrusion alarms, exit door controls, external alarms.
- **Video Patrol of Public Areas:** parking areas, Main entrance/exit gates, Traffic Control.
- **Criminal Investigations (carried out by An Garda Síochána):** robbery, burglary and theft surveillance.

## 7. COVERT SURVEILLANCE

NCTC will not engage in covert surveillance. Where An Garda Síochána requests to carry out covert surveillance on NCTC premises, such covert surveillance may require the consent of a judge. Accordingly, any such request made by An Garda Síochána will be requested in writing and the centre will seek legal advice.

## 8. NOTIFICATION - SIGNAGE

The Manager will provide a copy of this CCTV Policy on request to staff, learners, parents/Guardians and visitors to the centre. This policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use. The location of CCTV cameras will also be indicated to the Board of Management. Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to NCTC property. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

Appropriate location signage will include:

- At entrances to premises i.e. external doors and gates
- Reception area

- Main Hall



Images are being monitored and recorded for crime prevention, the prevention of anti-social behaviour, the prevention of bullying, for the safety of our staff and learners and for the protection of NCTC and its property. These images may be passed on to An Garda Síochána. This scheme is controlled by NCTC and operated by NCTC.

For more information contact: The Manager, Nenagh Community Training Centre, Johns Lane, Nenagh, Co. Tipperary

*Accordingly, the images captured by the CCTV system will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in context of an investigation/prosecution of that issue.*

## 9. STORAGE & RETENTION

Section 2(1) (c) (iii) of the Data Protection Acts states that data “shall not be kept for longer than is necessary for” the purposes for which it was obtained. A data controller needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue - such as a break-in or theft and those images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Manager. The Manager may delegate the administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be

viewed by other individuals to achieve the objectives set out above (such individuals may include the Gardaí, the acting Manager, other members of Instructing staff, representatives of the TETB, representatives of the HSE/or the parent of a recorded learner). When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

Tapes/DVDs will be stored in a secure environment with a log of access to tapes kept. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

## 10. ACCESS

Tapes/DVDs storing the recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to tapes/images will be maintained. Access to the CCTV system and stored images will be restricted to unauthorised personnel only i.e. Manager.

In relevant circumstances, CCTV footage may be accessed:

- By An Garda Síochána where NCTC (or its agents) are required by law to make a report regarding the commission of a suspected crime; or
- Following a request by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on NCTC property, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To assist the Manager in establishing facts in cases of unacceptable learner behaviour, in which case, the parents/guardians will be informed; or
- To data subjects (or their legal representatives), pursuant to access request where the time, date and location of the recordings is furnished to NCTC, or,
- To individuals (or their legal representatives) subject to a court order, or,
- To NCTC insurance company where the insurance company requires same to pursue a claim for damage done to the insured property.

**Requests by An Garda Síochána:** Information obtained through video monitoring will only be released when authorised by the Manager following consultation with the Chairperson of the Board of Management. If An Garda Síochána request CCTV images for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request

made by An Garda Síochána should be made in writing and NCTC should immediately seek legal advice.

**Access requests:** On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that other persons are not identified or identifiable. To exercise their right to access, a data subject must make an application in writing to the Manager of NCTC Or/And Chairperson (Nenagh Community Training Centre, Johns Lane, Nenagh, Co. Tipperary). The Centre may charge up to €6.35 for responding to such a request and must respond **within 40 days**.

## 11. RESPONSIBILITES

The Manager will:

- Ensure the use of CCTV systems is implemented in accordance with this Policy.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within NCTC.
- Ensure all existing CCTV monitoring at NCTC will be evaluated for compliance with this Policy.
- Ensure that CCTV monitoring at NCTC is consistent with the highest standards and protections.
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this Policy.
- Maintain a record of access (i.e. a log) to or the release of tapes or any material recorded or stored in the system.
- Ensure that monitoring recorded tapes are not duplicated for release.

- Ensure that the perimeter of view from fixed location cameras conforms to this Policy.
- Approve the location of temporary cameras to be used during special events that have security requirements and ensure their withdrawal following such events.  
*Note: Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by An Garda Síochána.*
- Consider both learners and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the centre and be mindful that no such infringement is likely to take place.
- Co-operate with the Health & Safety Officer (Manager) of NCTC in reporting on the CCTV system in operation in the centre
- Ensure that the external cameras do not intrude into the privacy of neighbouring residential housing and comply with the principle of “Reasonable Expectation of Privacy”.
- Ensure that monitoring tapes are stored in a secure place and that only authorised personnel are permitted access.
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Chairperson of the Board.

- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy.
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.
- Ensure that where An Garda Síochána request to set up mobile video equipment for criminal investigations, legal advice had been obtained and such activities have the approval of the Chairperson of the Board

## **12. IMPLEMENTATION & REVIEW**

The policy will be reviewed and evaluated from time to time. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, An Garda Síochána, Department of Education and Skills, Audit units (internal and external to the Centre) national management bodies, legislation and feedback from parents/guardians, learners, staff and others).

The date from which the policy will apply is the date of adoption by the Board of Management. Implementation of the policy will be monitored by the Manager.

## **APPENDIX 1- DEFINITIONS**

**Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;**

**CCTV-** Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.

**The Data Protection Acts** - The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All centre staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation

**Data-** information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

**Personal Data** - Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

**Access Request** - this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.

**Data Processing** - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,
- Disclosing the data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data.

**Data Subject** - an individual who is the subject of personal data.

**Data Controller** - a person who (either alone or with others) controls the contents and use of personal data

**Data Processor** - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data during their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection Acts place responsibilities on such entities in relation to their processing of data.