CLOSED CIRCUIT TELEVISION (CCTV) POLICY

Current version:	**V 2**
Last reviewed:	**June 2024**
Next review date:	**June 2025**
Person responsible for review:	**General Manager**

Introduction

This Policy explains the management, operation and use of the closed-circuit television (CCTV) system at Frankston District Netball Association Inc. (FDNA).

This policy applies to the installation of CCTV cameras on FDNA managed sites, and the use and disclosure of any footage produced by those cameras.

This policy is consistent with:

- Surveillance Devices Act 1999
- the Association's Risk Management policy.
- Victorian Privacy law.

FDNA has an obligation to ensure the netball courts are safe and secure, and fulfil a duty of care to staff, members and visitors. The CCTV system exists to assist the Association to fulfil these obligations and to prevent and manage other inappropriate behaviour on FDNA sites.

CCTV provides enhanced capability to protect FDNA's assets against vandalism and theft. CCTV strengthens FDNA's security by providing an appropriate level of surveillance at FDNA facilities and assists the Association to take all reasonable steps to prevent reasonably foreseeable (duty of care) incidents. The presence of CCTV cameras deters misconduct and inappropriate behaviour and reassures members, staff and visitors that they have some protection in FDNA facilities.

This policy describes how our CCTV system does this, consistent with Victorian privacy law.

CCTV Policy

Use of CCTV

Consistent with FDNA's obligations set out above, FDNA may use CCTV cameras to:

1. Prevent and verify incidents involving,

- Criminal behaviour - of anyone on site
- Staff misconduct.
- Other inappropriate behaviour - including of players, officials, visitors or members of the public. For example, this means the Association may use CCTV footage of incidents to help inform decisions about incident management.

2. Verify other incidents - involving members, staff and visitors (e.g. incidents in which a person has sustained injury, loss or damage on site).

3. To provide the Operations Manager with visual coverage during emergencies.

CCTV cameras are NOT:

- Hidden or covert.
- Located in private areas such as toilets, changing rooms or staff rooms.
- Used to monitor staff work performance.

Location of CCTV cameras

CCTV cameras are located in:

- Indoor Stadium foyer and hallways
- Cafe
- Indoor netball courts & some rooms such as function/meeting spaces
- Outside main stadium entrance, surrounding terrace and carpark

A notice is located near the stadium entry which alerts people to the presence of cameras and this CCTV Policy.

Access to CCTV footage

CCTV footage is only accessed for the purposes set out in this policy (see 'Use of CCTV footage') and only by the following people:

- The General Manager or nominee, including people explicitly authorised by the General Manager (Appendix 1).
- Any other people permitted by law.

Showing Footage To People Involved In Incidents

When using CCTV for the purposes listed in this policy under the heading 'Use of CCTV' and only when appropriate, the General Manager or nominee may elect to show specific footage of an incident to those directly involved, including relevant staff, members on request, where it doesn't impact the privacy of others.

Any person on FDNA premises may be captured on CCTV footage, of an incident that the General Manager may subsequently show to staff, members and/or any other people permitted by law (e.g Police)

Any requests for a copy of CCTV footage must be made via the Freedom of Information Act.

Managing and securing the CCTV system

The General Manager is responsible for ensuring the approved security company are appropriately managing and securing the CCTV system including:

- Operation of the CCTV system and ensuring it complies with this policy.
- Considering the appropriate location and use of cameras and method for storing CCTV footage.
- Maintaining and upgrading cameras when required.

Ownership of CCTV footage

FDNA owns the CCTV systems and CCTV footage.

Disclosure of CCTV footage

FDNA may only disclose CCTV footage externally as described in this policy or otherwise when permitted by law.

Storage of footage

CCTV footage is generally kept for no more than 28 days. If the Association has not used CCTV footage in any of the ways set out above, and there has been no request to view or access footage during this period, the footage is deleted.

Where CCTV footage has been used to verify an incident or where it is required to be retained for legal reasons, FDNA will manage and securely retain the footage.

It must be:

- Locatable (that is, the records are identifiable, their location is known, and they are retrievable).
- Secure from unauthorised access.
- Preserved so that they may be used for the duration of their retention period.

Implementation

This policy is available on the FDNA website under the policies section.

Recordings or images extracted from CCTV footage are kept securely in one place, accessible only to authorised persons only for purposes specified in this policy.

The General Manager or nominee, including people explicitly authorized, (Appendix 1), are not to forward recordings or images extracted from CCTV footage onto any person who is not a nominee or explicitly authorised (Appendix 1).

Any person requesting recorded footage will be referred to this policy

Supporting Documentation:

- Surveillance Devices Act 1999
- Privacy and Data Collection Act 2014
- Freedom of Information Act 2009

Appendix 1

FDNA access to CCTV Footage

CCTV footage is only accessed for the purposes set out in CCTV Policy and only by the following people:

- General Manager
- Operations Manager
- Hearings Officer/Complaint Manager
- Hearing(s) Tribunal panel members
- Security firm engaged by FDNA
- Anyone else required by law