



Man O'War GFC

Closed Circuit TV Policy

Created By	MOW Executive
Status	Approved
Version	1.0
Date	March 2025

1. Policy on CCTV Systems and Data Management

The Closed-Circuit Television System (CCTV) is installed in Man O'War GFC Club under the remit of the Executive Committee.

2. Purpose of the Policy

The purpose of this policy is to regulate the use of CCTV and its associated technology in the monitoring of the environs of premises under the remit of the Executive Committee of Man O'War GFC.

3. Purpose of the CCTV System

The CCTV system is installed internally and externally in premises for the purpose of enhancing security of the external and internal areas of the building, gym, carpark, and its associated equipment. As well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation to deter bullying, crime, vandalism and theft, as an aid to Health and Safety and to the discharge of the club's duty of care within and/or in the external environs of the premises at all times.

4. Scope of this policy

This applies to all personnel in and visitors to Man O'War GFC. It relates directly to the location and use of CCTV, the monitoring, recording and subsequent use of such recorded material.

General Principles

The Executive Committee of Man O'War GFC as the executive body, has a statutory responsibility for the protection of the club property and equipment as well as providing a sense of security to its employees, volunteers, members, visitors, and invitees to its premises. Man O'War GFC owes a duty of care under the provision of Health, Safety and Welfare legislation and utilises CCTV systems and its associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life in Man O'War GFC by integrating the best practices governing the surveillance of its premises, including using any evidence obtained in any disciplinary issue.

The primary aim of the CCTV monitoring of Man O'War GFC premises is to deter crime and vandalism and to assist in the protection and safety of the said property and its associated equipment and materials.

Monitoring for security purposes will be conducted in a professional, ethical, and legal manner and any diversion of the use of CCTV security technologies and personnel for other purposes is prohibited by this policy.

Any remote accessing of CCTV footage is strictly prohibited.

Information obtained through video monitoring may only be released when authorised by the Chairperson of the Executive Committee.

CCTV monitoring of public areas, for security purposes, will be conducted in a manner consistent with all existing policies adopted by the Executive Committee including the provisions set down in Equality and other Sports & Education related legislation.

The industry code of practice for video monitoring prohibits monitoring based on the classifications contained in Equality and other related legislation e.g., gender, marital status, family status, sexual orientation, religion, age, disability, race, or membership of the Traveller community.

Video monitoring of public areas, for security purposes, within the said establishment, is limited to areas that do not violate the reasonable expectation to privacy as defined by law.

Data from the CCTV system will only be accessed and used in accordance with Data Protection Regulations.

CCTV camera locations

Cameras are located in the following areas:

Internal

- The main stairs area accessing the first floor (1 camera)
- 1st floor open plan multipurpose area / gym area. (3 cameras)

External

- The front of building covering main door entry and carpark. (1 camera)

Employees, Members, and parents/guardians will be informed of the location and purpose of the CCTV system as outlined above. The right to access images captured by CCTV cameras shall be in accordance with the Data Protection Acts 1988, 2003 & the General Data Protection Regulation EU/2016/679 which confer rights on individuals as well as additional responsibilities on those persons and organisations processing any personal data.

Example of signage around premises.



5. Data Protection

All personal data recorded and stored by the CCTV system is governed by the Data Protection Acts of 1998, 2003 & the General Data Protection Regulation EU/2016/679. Under the Data Protection Acts a data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information in manual files or in a computerised form. The data controller in respect of images recorded and stored by the CCTV system in the club is the Chairperson/data protection officer on behalf of the Executive Committee.

The personal data recorded and stored by the CCTV system will only be available to the data controller and will be used only for the purposes outlined on the signage and within this policy.

6. Requests from individuals for personal data

(Please also refer to Man O'War GFC Data Protection policy)

Individuals whose images are recorded and stored by the CCTV system shall have the right to request and receive a copy of personal data processed by the system. Such requests shall be made in writing to the data controller and shall be complied with within a maximum of 28 days. Personal data recorded by the CCTV system shall be retained for a maximum of 30 days. Thereafter it will be deleted automatically.

The recorded footage and the monitoring equipment shall be securely stored in the secured server rack area located in the clubhouse area. **Unauthorised access to that system is not permitted at any time.**

7. Requests of disclosures by third parties.

No images from CCTV cameras will be disclosed to any third party without the express permission being given by the Chairperson of the Executive Committee and will only be disclosed to a third party in accordance with Data Protection Laws.

The following procedure shall be followed in the event that An Garda Síochána seeks to view or take a copy of CCTV footage from the clubs CCTV systems:

1. The data controller shall satisfy himself/herself that there is an investigation underway.
2. A request from An Garda Síochána must be made in writing on Garda headed notepaper. All CCTV systems and associated equipment will be required to be compliant with this policy.

8. Responsibilities:

The Executive Committee will:

- Ensure that a policy is in place, compliant with the relevant legislation, to govern the use of CCTV in the club.
- Ensure this policy is reviewed regularly by the Executive Committee
- Ensure this policy is made available to all members of the club

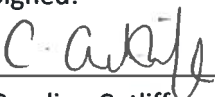
The Chairperson/ Data Protection Officer will:

- Act as Data Controller on behalf of the Executive Committee.
- Ensure that the use of the CCTV system is used in accordance with the policy set down by the Executive Committee and also in accordance with Data Protection regulations.

- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the club grounds.
- Ensure a DPIA (Data Protection Impact Assessment) is conducted regarding the installation of CCTV monitoring systems.
- Ensure that all CCTV monitoring systems are compliant with this policy.
- Be responsible for the release of any information or material in compliance with this policy.
- Maintain a record of the release of any material recorded or stored on this system.
- Provide a list of the CCTV cameras, their locations and the associated monitoring equipment and the capabilities of such equipment to the Executive Committee for formal approval.
- Approve the location of any temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events.
- Ensure that all areas being monitored are not in breach of a reasonable expectation of the privacy of individuals within the club.
- Advise the Executive Committee to ensure that adequate signage, at appropriate and prominent locations, is displayed.
- Ensure that external cameras are not intrusive in terms of their positions and views of residential housing and comply with the principle of "reasonable expectation of privacy".
- Ensure that recorded material is retained for a period of not longer than 60 days and will be erased unless required as part of a criminal investigation or court proceedings, criminal or civil, or other bona fide use as approved by the Executive Committee.
- Ensure that monitors are stored in a secure place with access by authorized personnel only.
- Report any breaches of this policy to the Executive Committee.

The club's Executive Committee will be responsible for ensuring the guiding principles outlined in this policy are implemented and followed by all club members.

Signed:


 Caroline Cutliffe
 Chairperson


 Tom Hoare
 Secretary

Date: 18.3.25

Date: 18/03/2025

---o0o---

APPENDIX 1 –GLOSSARY

TERM	DEFINITION
Data	Information in a form that can be processed. It includes both automated and Manual data
Automated Data	Any information on computer or information recorded with the intention of putting it on a computer. It includes not only structure databases but also e- mails, office documents and or CCTV footage/images
Manual Data	Information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system–this includes temporary folders.
Data Controller	A person who (either alone or with others) controls the contents and use of personal data. A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or, in structured manual files.
Data Processor	A person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment. If an organisation or person holds or processes personal data, but does not exercise responsibility for or control over the personal data, then they are deemed to be a "data processor".
Data Protection Officer (DPO)	An appointed officer with responsibility for the Data Protection compliance of the organisation.
Data Subject	A data subject is an individual who is the subject of personal data that is held
GPDR	The new EU General Data Protection Regulation (GDPR)-Regulation 2016/679 which comes into effect in May 2018 and replaces the current Data Protection Directive95/46/EC and the Irish Data Protection Act(s).
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
Sensitive Data	Any personal data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership
Processing	Processing means performing any operation or set of operations on data, including: <ul style="list-style-type: none"> •Obtaining, recording, or keeping data. •Collecting, organising, storing, altering, or adapting the data. •Retrieving, consulting, or using the data. •Disclosing the information or data by transmitting. •Disseminating or otherwise making it available; Aligning, combining, blocking, erasing, or destroying the data

