NORTHWEST KILMARNOCK BOWLING CLUB

CCTV POLICY

Introduction

The Club recognises that Closed Circuit Television (CCTV) systems can be intrusive to privacy.

For this reason, the Club has carried out a data protection impact assessment with a view to evaluating whether the CCTV system in place is a necessary and proportionate means of achieving the objectives set out below.

The result of the data protection impact assessment has informed the Club's use of CCTV and the contents of this policy.

Review of this policy shall be repeated regularly, and whenever new equipment is introduced, a review will be conducted, and a risk assessment put in place. We aim to conduct reviews not less than once every three years.

Objectives

The purpose of the CCTV system is to assist the Club in reaching these objectives:

(a) To protect members, staff, and visitors against harm to their person and/or property.

(b) To increase a sense of personal safety and reduce the fear of crime.

(c) To protect the Club buildings and assets.

(d) To support the police in preventing and detecting crime.

(e) To assist in identifying, apprehending, and prosecuting offenders.

(f) To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence

(g) To assist in managing the Club.

Purpose Of This Policy

The purpose of this policy is to regulate the management, operation, and use of the CCTV system at the Club. The CCTV system used by the Club comprises the following:

CAMERA TYPE	LOCATION	SOUND	RECORDING CAPACITY	SWIVEL / FIXED
Vari-Focal bullet network camera	In Bar	N	Y	F
Vari-Focal bullet network camera	In Corridor outside Bar	N	Y	F
Vari-Focal bullet network camera	In Committee Room	N	Y	F

Vari-Focal bullet network camera	External facing car park above defibrillator cabinet	N	Y	F
Vari-Focal bullet network camera	External facing bin store area	N	Y	F
Vari-Focal bullet network camera	External facing entrance gate	N	Y	F
Vari-Focal bullet network camera	External facing main entrance door	N	Y	F
Vari-Focal bullet network camera	External facing towards the green exit from Lounge area	N	Y	F

CCTV cameras are not installed in areas in which individuals would have a reasonable expectation of privacy such as toilets, changing facilities, etc.

CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant, so that members, staff, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

Statement Of Intent

Notification has been submitted to the Information Commissioner's Office (ICO) and the next renewal date has been recorded.

The CCTV system will seek to comply with the requirements of both the Data Protection Act 2018 and the most recent ICO Code of Practice.

The Club will treat the system, all information, documents, and recordings (both those obtained and those subsequently used) as personal data protected under the Data ProtectionAct 2018 and will process such data in accordance with this CCTV Policy and the Club's Privacy Policy.

The system has been designed so far as possible to avoid observation of adjacent private homes, gardens, and other areas of private property.

Materials or knowledge secured because of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design have endeavoured to ensure that the system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the ICO will be clearly visible on the site and make clear who is responsible for the equipment.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

CCTV images are not retained for longer than necessary, considering the purposes forwhich

they are processed. Data storage is deleted from the system after a period of 30 days.

Recorded images will only be retained long enough for any incident to come to light (e.g., for a theft to be noticed) and the incident to be investigated. In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 30 days.

System Management

Access to the CCTV system and data shall be password protected and will be kept in a secure area.

The CCTV system will be administered and managed by the System Manager, currently the Data Protection Lead, who will take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the System Manager the system will be managed by the Committee.

The system and the data collected will only be available to the System Manager, and appropriate members of the Committee. The cameras can be accessed via a smart phone.

The CCTV system is designed to be in operation 24 hours each day, every day of the year, though the Club does not guarantee that it will be working during these hours.

The System Manager will check and confirm the efficiency of the system regularly and that the equipment is properly recording and that cameras are functional.

Cameras have been selected and positioned to best achieve the objectives set out in this policy by proving clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those specified above requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused.

Details of all visits and visitors for access to the CCTV system will be recorded in a system logbook including time/data of access and details of images viewed and the purpose for so doing.

Downloading Captured Data to Other Media

To maintain and preserve the integrity of the data (and to ensure their admissibility inany legal proceedings) any downloaded media used to record events from the hard drive must beprepared in accordance with the following procedures: -

(a) Each downloaded media must be identified by a unique mark.

(b) Before use, each downloaded media must be cleaned of any previous recording.

(c) The System Manager will register the date and time of downloaded media insertion, including its reference.

(d) Downloaded media required for evidential purposes must be sealed, witnessed, and signed by the System Manager, then dated and stored in a separate secure evidence store, currently the Safe. If a downloaded media is not copied for the police before it is sealed, a copy may be made later providing that it is then resealed, witnessed, and signed by the System Manager, then dated and returned to the evidence store.

(e) If downloaded media is archived the reference must be noted.

(f) If downloaded media is put onto a device, the device will be encrypted, and password protected.

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her replacement, and other authorised Committee members. However, whereone of these people may be later called as a witness to an offence and where the data contentmay be used as evidence, it shall be preferable, if possible, for that person to withhold viewing the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the Club and downloaded media (and any images contained thereon) are to be treated in accordance with data protection legislation. The Club also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealedbag.

The police may require the Club to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely storeduntil they are needed by the police.

Applications received from outside bodies (e.g., solicitors) to view or release imageswill be referred to the Club's Data Protection Lead, and a decision made by the Committee in consultation with the Data Protection Lead.

Complaints About the Use Of CCTV

Any complaints in relation to the Club's CCTV system should be addressed to the Data Protection Lead or any Committee member.

Request For Access by The Data Subject

The Data Protection Act 2018 provides Data Subjects – those whose image has been captured by the CCTV system and can be identified - with a right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to the Data Protection Lead.

Public Information

Copies of this policy will be available on the Club website.

Policy	**CCTV**
Statutory Requirement	**Yes (all the while cameras are installed)**
Approved	**March 2022**
Responsible Officer	**System Manager**
Date of last review	**N/A**
Frequency of Review	**Every 3 years**
Date of next Review	**March 2025**