

**LINLITHGOW SPORTS CLUB**  
**CLOSED CIRCUIT TELEVISION POLICY**

**GENERAL**

**THE AIM OF THE POLICY**

The Closed-Circuit Television (CCTV) has been installed at the club and the system will be monitored to: -

- Provide security and safety for Club members, staff and visitors
- Provide security of the Club premises and equipment

It is recognized that images are sensitive material and subject to the General Data Protection Regulations (GDPR):

**DATA CONTROLLING OFFICER (DCO)**

The DCO is responsible for ensuring day to day compliance with this regulation, which includes on-going registration with the Information Office Commissioner.

The DCO will be nominated by the Board of Management.

**CCTV SITING**

- Corridors leading to the lounge and squash areas
- Squash area corridor
- Lounge, focused on the patio doors

Signs at all access doors to the club showing that CCTV is in operation.

**RECORDINGS**

- Digital recordings are made using digital video recorders operating in real time mode and are stored on either tape or hard drive, which will normally be retained for 30 calendar days from the date of recording, unless needed for further investigation.
- The CCTV System is a localized system and for internal use only. Remote access will only be available to the DCO and any personnel authorised by the DCO.

**ACCESS TO IMAGES**

Access to images will be restricted to the DCO except in the following circumstances: -

- Required by law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder.
- Required by prosecution agencies.

**LINLITHGOW SPORTS CLUB**  
**CLOSED CIRCUIT TELEVISION POLICY**

**GENERAL**

**ACCESS TO IMAGES**

- Required by emergency services in connection with the investigation of an accident.
- Required by anyone who believes that they have been filmed on CCTV can ask to see a copy of the images, subject to guidelines covered by the GDPR. They can request, in writing from the DCO access to the images and access must be allowed within 30 calendar days, the DCO will then arrange for a viewing of the images and subsequent discussion of content. The GDPR provides the DCO the right to refuse a written request, where such access could prejudice a criminal investigation or impede the apprehension or prosecution of offenders. If the DCO decides to refuse the request all reasons will be fully documented and the subject will be informed.