

Penryn Rugby Football Club

CCTV and Video Surveillance Policy

Effective Date: September 2026

Review Date: September 2027

Approved by: Penryn RFC Committee



1. Introduction

Penryn Rugby Football Club (PRFC) uses CCTV and video surveillance for legitimate safety and security purposes. The Club recognises that images of identifiable individuals are personal data and must be managed lawfully, fairly, transparently and securely.

This policy explains how PRFC manages CCTV in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and relevant guidance issued by the Information Commissioner's Office (ICO). Particular care will be taken where surveillance covers areas used by children and young people.

2. Policy Aims

The purpose of this policy is to:

- Protect players, members, staff, volunteers, visitors and members of the public.
- Protect Club buildings, grounds, equipment and other property.
- Help prevent and detect crime, theft, vandalism and anti-social behaviour.
- Assist with the investigation of incidents occurring on Club premises.
- Ensure CCTV is used only where necessary, proportionate and appropriate.
- Protect the privacy and data protection rights of individuals captured by the system.

3. Lawful Basis and Purpose

PRFC will identify and document an appropriate lawful basis for operating CCTV. For routine security CCTV, the Club will normally rely on its legitimate interests in protecting people and property and preventing or investigating crime and anti-social behaviour.

The Club will balance these interests against the rights and freedoms of individuals. CCTV collected for security purposes will not routinely be used for unrelated purposes or for general monitoring of employee or volunteer performance.

4. Camera Locations and Privacy

Cameras may be used at entrances and exits, external areas, car parks, bar and social areas, corridors, access points, storage areas and other locations where a genuine security or safety need has been identified.

Cameras will be positioned to avoid capturing more information than is reasonably necessary. Where practicable, views of neighbouring property and areas outside Club premises will be minimised.

CCTV will not be installed in toilets, changing rooms or shower areas, or other locations where individuals have a particularly high expectation of privacy.

5. Children and Young People

Because PRFC provides activities for children and young people, additional consideration will be given to their privacy and safeguarding.

CCTV covering areas regularly used by children will be limited to what is necessary for legitimate safety and security purposes. Footage involving children will only be accessed, copied or disclosed where there is a legitimate and lawful reason.

Any safeguarding concern identified through CCTV will be managed under the Club's safeguarding procedures and referred to the Club Safeguarding Officer and/or appropriate statutory authorities where required.

6. Audio Recording

The Club's CCTV system will not normally record audio. Where equipment includes microphones or audio functionality, this should normally be disabled.

Any proposal to introduce audio recording must be specifically justified and subject to an appropriate privacy assessment before activation.

7. CCTV Signage and Transparency

Clear signs will be displayed so that people are aware CCTV is in operation before, or as they enter, monitored areas.

Signs should identify Penryn Rugby Football Club as the organisation responsible for the system, explain the purpose of surveillance and provide an appropriate means of contacting the Club about CCTV or data protection matters.

8. Access to CCTV

Access to live and recorded CCTV will be restricted to persons specifically authorised by the Club.

Authorised users must:

- Access CCTV only where there is a legitimate reason.
- Maintain the confidentiality of recordings.
- Not copy, photograph or share footage using personal devices.
- Not publish or distribute footage through social media or messaging applications.
- Keep passwords and login details secure.
- Report suspected misuse or security breaches immediately.

Where practicable, access to recordings and exported footage should be logged.

9. Storage and Security

CCTV recordings will be stored securely and protected against accidental or unlawful loss, alteration, disclosure or access.

Appropriate controls may include strong passwords, restricted administrator privileges, secure recording equipment, network protection, encryption where appropriate and timely software or firmware updates. Manufacturer default passwords must be changed before equipment is placed into service.

10. Retention of Recordings

CCTV footage will be retained only for as long as necessary for the purpose for which it was collected. The Club's standard retention period should be documented within its CCTV operating procedures and periodically reviewed.

Relevant footage may be retained beyond the normal period where necessary for an incident, safeguarding matter, insurance claim, disciplinary process, legal proceedings or police investigation. Such footage will be retained only for as long as reasonably necessary.

11. Disclosure of Footage

CCTV images will not normally be disclosed to third parties. Lawful disclosure may include the police or other law-enforcement bodies, emergency services, insurers, legal advisers, safeguarding authorities, courts or tribunals, and individuals exercising their data protection rights.

Before footage is released, the Club will consider the lawful basis for disclosure and whether images of other identifiable individuals need to be obscured. Significant disclosures should be recorded.

12. Police Requests

Where police request CCTV footage, authorised Club personnel should verify and record the request. Records should include the requesting officer's details, police force, incident or crime reference where available, date and time, footage requested, reason for the request and what was supplied.

Footage should be transferred securely. A police request does not automatically justify unrestricted access to the Club's CCTV system.

13. Subject Access Requests

Individuals may have the right to request copies of CCTV images containing their personal data. Requests should provide enough information for the Club to locate the footage, such as the date, approximate time and location.

Requests will normally be handled within one calendar month, subject to applicable data protection provisions and exemptions. Where recordings contain other

identifiable individuals, the Club will consider whether those individuals should be obscured before disclosure.

14. Use of CCTV in Incidents and Disciplinary Matters

CCTV is primarily operated for safety, security and crime-prevention purposes. Where footage legitimately obtained for those purposes reveals serious misconduct, a safeguarding concern or a breach of Club rules, the Club may consider whether use of that footage in an investigation is lawful and proportionate.

CCTV will not routinely be used as a means of monitoring employees, volunteers, coaches or members.

15. CCTV and Social Media

CCTV recordings are security information and must not be treated as general photography or promotional material.

Footage must not be posted on Facebook, Instagram, WhatsApp, the Club website or other social media by Club officials, staff or volunteers unless there is an exceptional, lawful and specifically authorised reason. Club publicity images should normally be obtained through the Club's photography and media consent arrangements.

16. Data Breaches

Any loss, unauthorised disclosure, unauthorised access or misuse of CCTV footage must be reported immediately to the Club's designated data protection contact.

The Club will assess the incident under its data breach procedures and determine whether notification to the ICO and/or affected individuals is required.

17. Data Protection Impact Assessment

PRFC will consider whether a Data Protection Impact Assessment (DPIA) is required when introducing or significantly changing CCTV.

A DPIA will be undertaken where surveillance is likely to result in a high risk to individuals' rights and freedoms. Particular consideration will be given before introducing facial recognition, biometric identification, ANPR, systematic large-scale monitoring, audio recording or other intelligent or AI-based surveillance technologies.

18. Maintenance and Review of the System

The Club will periodically check camera operation and positioning, recording functionality, image quality, date and time accuracy, storage and overwrite operation, user access, passwords, software or firmware and CCTV signage.

The need for each camera and the overall CCTV system will be periodically reviewed to ensure surveillance remains necessary and proportionate.

19. Responsibility

Overall responsibility for CCTV rests with the Penryn RFC Committee. Day-to-day responsibility may be delegated to authorised Club officers or personnel.

Only persons authorised by the Committee may administer the CCTV system or access recorded footage.

20. Complaints

Anyone with concerns about the operation of the Club's CCTV system should initially contact Penryn Rugby Football Club through the Club's published contact details.

Complaints will be considered appropriately and individuals may also raise data protection concerns with the Information Commissioner's Office.

21. Policy Review

This policy will be reviewed at least annually and sooner where the CCTV system is substantially changed, new surveillance technology is introduced, the purpose of surveillance changes, a significant incident identifies shortcomings, or relevant legislation or regulatory guidance changes.

Approved by Penryn RFC Committee

Chair: _____

Signature: _____

Date: _____



PENRYN
❖ BOROUGH RUGBY ❖