



# **CCTV Policy Guidelines**

## **Privacy policy**

### **Introduction**

Folkestone Rugby Football Club (FRFC) is fully committed to the safety of its staff, members and visitors and to this extent has invested in the security of its buildings and facilities. The purpose of this Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at FRFC.

Common CCTV systems are based around digital technology and therefore need to be treated as information that will be processed under the Data Protection Act 1998. The person ultimately responsible for data protection within Folkestone Rugby Football club (FRFC) is the Data Protection Officer (DPO). He/she will be the data controller and has the most responsibility when it comes to protecting the privacy and rights of the data's subject, such as the user of a website or CCTV images. The data controller controls the procedures and purpose of data usage. The data controller will dictate how and why data is used by the organisation.

The CCTV system comprises of numerous dome cameras located both internally and externally around the Club. These cameras will have infra-red capability. All cameras may be monitored live and are only accessible to approved members of staff/committee. Some of the cameras may also have the capability to record sound.

The CCTV system is owned by FRFC and will be subject to review annually. All images will be recorded and stored on a Digital recorder for a period of approximately 30 days when they will be automatically overwritten. The recorder has the capability to permanently save an incident or remove it to a memory stick.



## **Objectives of the CCTV System**

The objectives of the CCTV system are: –

- To protect the Club buildings and its assets to ensure they are kept free from intrusion, vandalism, damage or disruption.
- To increase the personal safety of staff, members and visitors and reduce the fear of physical abuse, intimidation and crime.
- To support the police in a bid to deter and detect crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To protect members of the public and private property.
- To assist in the usage and management of the Club building on a day-to-day basis.

## **Statement of Intent**

The Club will comply with the Data Protection Act 1998, whether it be information, recordings and downloads which relate to the CCTV system.

Cameras will be used to monitor activities within the Club buildings, the car parks and other areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the occupants within the club, together with its visitors.

Unless an immediate response to events is required, staff will not direct cameras at an individual, their property or a specific group of individuals, without an authorisation from the Data Protection Officer or club officer being obtained. The system will not be open but password protected.

Materials or knowledge secured as a result of the CCTV system will not be used for any commercial purpose. Downloads will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Downloads will never be released to the media for purposes of entertainment.

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



Warning signs, as required by the Code of Practice of the Information Commissioner will be placed at all access routes to areas covered by the Club CCTV.

### **Operation of the System**

The system will be administered and managed by the Data Protection Officer, in accordance with the principles and objectives expressed in this Policy.

The CCTV system will be operated 24 hours each day, every day of the year. (24/365)

### **CCTV System**

The DPO will check and confirm the efficiency of the system on a regular basis and that the equipment is properly recording and that cameras are functional. Any faults will be reported immediately to the Club Secretary.

Access to the CCTV will be strictly limited to nominated members of staff/Committee approved by the Club Officers. This access will be password protected to limit unwarranted access. Passwords will be single issue so that a log can be kept of access.

Unless an immediate response to events is required, staff must not direct cameras at an individual or a specific group of individuals.

The CCTV system may generate a certain amount of concern from members of the public. Any concern expressed by a member of the public should be referred to the DPO. If permission is granted by the DPO or club officer, the member of the public must be accompanied throughout the visit by a member of staff.

Any site visit by a member of the public may be immediately curtailed if the operational requirements of the CCTV System make this a necessity.

Other administrative functions will include maintaining hard disc space, filing, and maintaining occurrence and system maintenance logs by the DPO. The system will have the capability to be viewed remotely on a SMART Device. Similarly, this will be strictly controlled.



In the event of an emergency, which requires an immediate contact with an emergency service, that emergency service will be contacted by a member of staff.

### **Liaison**

Liaison meetings may be held with all bodies involved in the support of the CCTV system i.e. maintenance contractors, approved staff, police etc.

### **Monitoring Procedures**

Camera surveillance may be maintained at times for monitoring purposes.

### **VEO Rugby Sports Camera**

FRFC owns and uses a portable Veo Sports Camera and self-contained battery pack and camera recording system. It can be sited on a raised tripod, adjacent to the playing area and can record play during a match or training sessions. This is predominantly to assist with the improvement of performance and to assist coaches identifying issues. It can focus on individuals or give a general playing overview.

Inevitably it may also record incidences of foul or play or ancillary incidences away from the field of play that may subsequently be deemed criminal conduct. Any product from this recording will be saved and passed to the DPO. The only exception being that it will only be accessed by the Club Coach and or/Director of Rugby. Any incidences of foul or potential criminal conduct **will not** be uploaded to the web but retained for later scrutiny or secured as evidence for the authorities. The same guidelines as for CCTV image recovery will be adhered too.

### **Video Download Procedures**

Recordings may be viewed by the police and authorised officers from the Police for the prevention and detection of crime. Permission to do this will be given by the DPO. Any request for images to be captured will be subject to a Data Protection Act Request form, duly signed by the appropriate senior police officer.



A record will be maintained of the release of downloads to the police or other authorized applicants. A register will be available for this purpose and will be kept by the DPO.

Viewing of downloads by the police must be recorded in writing and in the register. Requests by the police can only be actioned under section 29 of the Data Protection Act 1998.

Should a download be required as evidence, a copy may be released to the police under the procedures described in the above paragraphs of this Policy. Downloads will only be released to the police on the clear understanding that any copy or reproduction remains the property of the Club, and both the copy and information contained in it are to be treated in accordance with this Policy. The Club also retains the right to refuse permission for the police to pass to any other person the copy or any part of the information contained thereon.

Applications received from outside bodies (e.g. Solicitors) to view or release downloads will be referred to the DPO. In these circumstances' downloads will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee of £150,00 can be charged in such circumstances. The club solicitor will be consulted on all requests.

### **Breaches of the Policy (including breaches of security)**

Any breach of this Policy by Club staff will be initially investigated by the Club Secretary, for him/her to take the appropriate disciplinary action.

Any serious breach of the Policy will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach.

### **Assessment of the Scheme and CCTV Usage Policy**

Performance monitoring, including random operating checks, may be carried out by the approved persons.

### **Complaints**

Any complaints about the Club's CCTV system should be addressed to the Club Secretary.



Complaints will be investigated in accordance with Section 9 of this Policy.

### **Access by the Data Subject**

The Data Protection Act provides Data Subjects (individuals to whom “personal data” relate) with a right to data held about themselves, including those obtained by CCTV.

Requests for Data Subject Access should be made in writing to the DPO.

### **Public Information**

Copies of this Policy will be available to the public, by making a request to the Club Secretary.

A copy of this Policy will be located in the Club House for information purposes to members of staff.

### **System Maintenance and Monitoring**

The system will be maintained in accordance with the Data Protection Act 1998.

The system will only be maintained and monitored by companies which carry the relevant accreditation from the Security Systems and Alarm Inspection Body (SSAIB) or National Security Inspection (NSI).

It will be the responsibility of the DPO to liaise with the maintaining company for the reporting of faults on the system, any changes to the site which may affect the operation of the system.

It will be the responsibility of the DPO to arrange regular system reviews with the maintaining company.

### **Summary of Key Points**

- This CCTV Usage Policy will be reviewed on an annual basis.
- The CCTV system is owned and operated by the Club.
- The CCTV system cannot be accessed by visitors/members of the public except by prior arrangement with the DPO and with good reason. The reason must be recorded.



- Liaison meetings may be held with the police and other bodies.
- Copies of downloads may only be viewed by authorised staff and the police and with the express permission of the DPO.
- Copies required as evidence will be properly recorded witnessed and packaged before copies are released to the police. It is essential that the evidence trail is carefully adhered to, and training will be given to ensure proper procedure is adopted.
- Copies will not be made available to the media for commercial or entertainment reasons.
- Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with the CCTV Usage Policy.
- Any breaches of this Policy will be investigated by the DPO: an independent investigation will be carried out for serious breaches.
- Breaches of the Policy and recommendations will be reported to the DPO.
- The system will be maintained on a regular basis by an approved contractor.

**Further information and queries should be directed to the Data Protection Officer via Folkestone Rugby Club.**

