

## **Crosby & District Scouts CCTV Policy Introduction**

Crosby & District Scout Council (CDSC) has installed closed-circuit television (CCTV) systems at Crosby & District Scouts Headquarters (DHQ) to help maintain a safe and secure environment for young people, volunteers, and to protect District property.

This policy outlines the acceptable use, management, and access procedures for CCTV systems and footage, in compliance with:

- General Data Protection Regulation (GDPR)
  - Data Protection Act 2018
  - Human Rights Act 1998
  - Protection of Freedoms Act (POFA) – Surveillance Camera Code of Practice
  - Other relevant legislation and best practices
- 

### **Purpose**

The CCTV system is in place to:

1. Prevent and detect crime or misconduct
  2. Assist in identifying and prosecuting offenders
  3. Monitor the security of our premises
  4. Support compliance with health and safety procedures
  5. Provide evidence in investigations of unsafe or unauthorised activity
- 

### **Scope and Applicability**

This policy applies to all CCTV systems installed at CDSC properties and all individuals on site, including volunteers, visitors, and third-party contractors.

CCTV will not be used:

- For entertainment or broadcast purposes
- For covert surveillance, unless expressly authorised under legal grounds and with appropriate judicial oversight
- To capture or store biometric or automated recognition data (e.g. number plate recognition)

Footage will only be shared with authorised third parties such as law enforcement when legally required.

---

### **Responsibilities**

- CDSC Trustees: Hold overall accountability for CCTV policy compliance and legal adherence.
  - District Lead Volunteer (DLV) and Appointed Personnel: Oversee operational management of the CCTV system, including user access and maintenance.
  - Authorised Personnel: Access, manage, and review footage in accordance with this policy and their training. They are responsible for secure data handling and maintaining review logs.
- 

### **System Overview**

- The CCTV system operates 24/7 and includes fixed cameras, encrypted digital recorders, and secure remote monitoring.
  - Cameras are installed externally, covering entry and exit points.
  - No cameras are installed in private areas such as toilets, showers, or changing rooms.
  - Signage complies with ICO and Surveillance Camera Code of Practice requirements, informing individuals they are entering an area covered by CCTV.
  - Every effort is made to avoid capturing private residential spaces.
- 

### **System Access and Security**

- The CCTV system is connected via a secure hard-wired Ethernet network to an on-site Network Video Recorder (NVR).
- Data is encrypted, and access requires individual user credentials.
- The NVR is stored securely and has no permanently connected monitor.
- Live and recorded footage may be accessed remotely by authorised personnel only.
- A central log must be kept of any footage reviewed, including:
  - Name of reviewer
  - Date, time, and location of footage
  - Reason for review

Version 1 September 2025.

Review Date Summer Trustees meeting 2026

### **Operator Training**

All personnel responsible for operating or reviewing CCTV footage will receive training on:

- Legal requirements
- Technical system use
- Proper handling and storage of recordings

This training is refreshed periodically and upon any system or policy updates.

---

### **Processing of Images**

- Access to footage is strictly limited to those authorised by the CDSC Trustees for the purposes set out in this policy.
  - All individuals with access to footage are bound by confidentiality and data protection obligations.
  - Screens must not be left visible to unauthorised individuals.
  - No footage should be saved to personal or local devices.
- 

### **Image Quality and Maintenance**

- Regular checks must ensure all cameras function correctly, are unobstructed, and capture images of sufficient resolution to support the system's stated purposes.
  - Environmental factors (e.g. lighting) will be managed to maintain image clarity.
  - Equipment must be protected from vandalism or accidental damage.
- 

### **Retention and Disposal of Footage**

- Recordings are retained on a rolling basis for approximately 14–21 days, and a maximum of 31 days.
- Footage will be deleted after the retention period unless required for legal or investigative proceedings.
- Footage saved beyond the standard retention period must be stored securely on CDSC's SharePoint system.

- Media stored on USB/CD must be deleted or securely destroyed within one month unless a longer retention is required by law enforcement.
- 

### **Data Protection**

- CDSC has completed a Data Protection Impact Assessment (DPIA) in accordance with the Surveillance Camera Code of Practice.
  - CCTV footage that can identify individuals is treated as personal data and is subject to GDPR.
  - CDSC is registered annually with the Information Commissioner's Office (ICO) under registration reference ZB858932.
- 

### **Subject Access Requests (SARs)**

Individuals have the right to request CCTV footage of themselves under GDPR. Requests must include:

1. Date and approximate time
2. Location of the camera
3. Description or image of the individual (if needed)
4. Proof of identity

SARs should be emailed to: [jennifer.wilson@crosbyscouts.org.uk](mailto:jennifer.wilson@crosbyscouts.org.uk)

- If footage contains third-party data, it may be obscured, or the request may be declined if fulfilling it would compromise the rights of others or interfere with legal processes.
  - SAR responses may take up to 60 calendar days for complex cases, in accordance with GDPR.
- 

### **Access by Law Enforcement and Third Parties**

Footage will only be disclosed to:

- Law enforcement agencies with a formal request
- Other third parties where legally obligated

Only the DLV or a CDSC Trustee may authorise such disclosures.

All disclosures will be logged, including:

Version 1 September 2025.

Review Date Summer Trustees meeting 2026

- Name of the requesting party
  - Date of the request
  - Footage reviewed
  - Name of the authorising individual
- 

### **Audit and Review**

This policy, and the CCTV system's technical and operational components, will be reviewed annually, or sooner if there are significant changes in:

- Legislation
- Technology
- Security needs

The review will ensure:

- Continued legal compliance
- Technical effectiveness
- Alignment with the stated purposes of CCTV use