



Cardiff West Community High School

CCTV Policy 2026-28

Created by: V. Evans

Approved by: A. Batten

Date: June 2026

Review: September 2027



1. Purpose of the Policy

This policy outlines the use of Closed-Circuit Television (CCTV) systems at Cardiff West CHS. The system is in place to:

- Enhance the safety and security of pupils, staff, and visitors
- Protect school buildings and assets
- Support the prevention, detection, and investigation of misconduct or criminal activity
- Assist in safeguarding and behaviour management

This policy operates alongside the school's Data Protection (GDPR) Policy.

2. Legal and Regulatory Framework

The school's use of CCTV complies with:

- UK GDPR and the Data Protection Act 2018
- Surveillance Camera Code of Practice (Protection of Freedoms Act 2012)
- ICO CCTV Guidance
- Human Rights Act 1998
- Welsh Government safeguarding expectations

3. Scope of the System

CCTV cameras are installed in selected internal and external areas of the school, including:

- Entrances and exits
- Corridors and communal areas
- External perimeters
- Car parks and access points

CCTV will not be used in areas where individuals have a reasonable expectation of privacy, including:

- Toilets
- Changing rooms
- Staff welfare areas (unless justified and risk-assessed)

4. Principles Governing Use

Cardiff West CHS ensures that CCTV use is:

- Necessary and proportionate to its purpose
- Transparent, with clear signage displayed across the site
- Fair and lawful, with due consideration of privacy rights
- Regularly reviewed to ensure continued justification

5. Purpose Limitation

Footage will only be used for:

- Safeguarding concerns
- Behaviour management and discipline
- Health and safety monitoring
- Crime detection and prevention
- Supporting investigations (internal or by authorities)

Footage will not be used for routine staff monitoring unless linked to a legitimate investigation.

6. Data Protection and GDPR Compliance

The Headteacher is the Data Controller for CCTV data.

- CCTV footage is considered personal data
- Processing is based on the lawful basis of public task and legitimate interests
- A Data Protection Impact Assessment (DPIA) has been completed
- Access to footage is strictly controlled

7. Storage and Retention

Footage is securely stored and retained for up to 30 days unless required for investigation.

Footage retained longer must be justified and documented.

8. Access to Footage

Access is restricted to authorised personnel, such as:

- Headteacher
- Designated safeguarding lead
- Senior leadership team (SLT) members with delegated responsibility
- Network manager (technical access only)

All access must be:

- Logged and auditable
- Justified and proportionate

9. Requests for Access

Individuals may request access to CCTV footage of themselves:

- Requests must be made in writing
- The school will respond within statutory timeframes
- Footage may be redacted or refused where it affects the rights of others

10. Sharing of Footage

Footage may only be shared:

- With law enforcement agencies where formally requested
- With safeguarding authorities where necessary
- In response to legal obligations

All disclosures are:

- Recorded
- Assessed for legality and proportionality

11. Signage and Transparency

Clear signage is displayed across the school.

12. Security of the System

Systems are password protected and secure.

13. Monitoring and Review

This policy will be:

- Reviewed annually
- Updated in line with changes in legislation or guidance
- Supported by periodic audits of CCTV usage and necessity

14. Roles and Responsibilities

Governing body, Headteacher, DPO, ICT Manager and safeguarding lead have defined roles.

Role	Responsibility
Governing Body	Oversight of policy compliance
Headteacher	Overall accountability
Data Protection Officer (DPO)	Compliance with data protection laws
Network Manager	Technical management and security
Safeguarding Lead	Use in safeguarding matters

15. Complaints

Concerns should be directed to the Headteacher or DPO.

Appendix A – Key Good Practice

- Regularly review camera locations and necessity
- Avoid excessive coverage or intrusive angles
- Ensure staff awareness and training
- Maintain clear audit trails for footage access

Appendix B – CCTV Data Protection Impact Assessment (DPIA)

Includes:

- Project overview
- Lawful basis
- Risks and mitigation
- Data retention
- Approval