Radyr Comprehensive School

Ysgol Gyfun Radur

Respect ◆ Commitment ◆ Success

CCTV Policy

REVIEWED: December 2025
NEXT REVIEW: December 2028

SIGNED:

_____ ___Dr D S (Chair of Governors)

____ ___Mr A D Williams (Headteacher)

DATE: 08.12.2025

CCTV POLICY

Introduction

The purpose of this policy is to set out the management, operation and use of the closed-circuit television (CCTV) system at Radyr Comprehensive School.

The School's CCTV systems comprises of **134** cameras located within and around the school buildings.

The monitoring and recording equipment is located at **IT Network Manager's office** and overall School officer in charge of the CCTV is Mr Paul Robinson

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images.

All employees are aware of the restrictions in relation to access to, and disclosure of recorded images.

This Policy has been drawn up to govern the management of all operations of CCTV devices and other recording devices which are subject to the provisions of the:

- Data Protection Act 2018
- ICO CCTV Code of Practice requirements
- Human Rights Act
- Home Office Surveillance Camera Code of Practice.

Purpose of processing CCTV:

The use of the systems operated by the School shall be for the purpose of:-

- Prevention and detection of crime
- Reducing the fear of crime
- Improving protection for staff, children and parents
- Improving the safety and security of residents, visitors and the business community who use the facilities
- Discouraging anti-social behaviour

Statement of intent

The CCTV system has been registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will comply with the

requirements both of the Data Protection Act 2018 and the associated Codes of Practices outlined within this policy.

The School **Must** confirm their CCTV is registered within their ICO registration prior to publication of this policy

The Head Teacher shall ensure that all appropriate staff are trained on the use of the equipment and are familiar with their data protection responsibilities

All devices operated are subject to Impact Assessments in line with the CCTV Code of Practice to ensure that they have legitimate purposes for processing in line with the requirements of the Data Protection Act 2018 and Article 8 of the Human Rights Act.

CCTV Warning signs, as required by the Code of Practices' will be placed around all areas of the School. These will clearly set out that CCTV is in operation, the owner of the system and contact details of the system owner.

Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated.

Storage and retention of footage

Footage will not be retained for longer than 31 days, unless an incident occurs which necessitates extraction and retention of said footage as evidence.

While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

All retained data will be stored securely.

Access to footage

Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available. Please refer to the CCTV protocol (available in the Network Manager's office)

Individual Right Requests

Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act 2018.

All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time

and location.

The school will respond to requests within 30 calendar days of receiving the written request

Access to and disclosure of footage to third parties

There will be no disclosure of recorded data to third parties other than to authorised organisations, such as the Police, where there may be a reasonably need to access the footage.

These requests will be documented under the Schedule 2 and 3 conditions of the Data Protection Act to ensure disclosures are lawful. Requests must be made in writing to the Head Teacher.

Footage may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

Complaints

Any complaints about the schools' CCTV system should be addressed to the Head Teacher.

Complaints will be investigated in accordance with this Policy.

CCTV Monitoring and Access Procedure

1. Governance and Responsibility

Role	Name	Responsibilities
Data Protection Lead	**Claire Jones**	Reviews Data Subject Access Requests (SARs).
CCTV Responsible Officer (RO)	**Paul Robinson**	Primary point of contact for all CCTV operations.
Deputy Responsible Officer (DRO)	**Paul Madell**	Assumes all RO responsibilities in Paul Robinson's absence.

2. Internal CCTV Footage Requests

This procedure is for staff-initiated requests to access CCTV footage for internal school incidents only.

2.1. Request Submission

- **Authorized Requesters:** Only members of the **Senior Leadership Team (SLT)** or a **Wellbeing Officer** are permitted to request footage.
- Submission Method: Requests must be submitted via the IT Support Helpdesk System by emailing: itsupport@radyr.net

- **Required Information:** The email request **must** be detailed and include:
    - **Area:** The specific location(s) covered by the camera.
    - **Date and Time:** The precise date(s) and time frame(s) of the incident (e.g., "14/11/2025, 11:45 to 12:05").
    - **Incident Description:** A clear, concise summary of the event requiring review.

2.2. Review, Access, and Security

1. **Review by RO:** The Responsible Officer (or Deputy) will review the system to locate the requested incident.
2. **Secure Storage (Clips):** If located, a video clip will be downloaded to a designated, **secure, password-protected network folder** with restricted access controls.
3. **Restricted Access:** Access to this secure folder is strictly limited to **SLT members** and **Wellbeing Officers** only for the specific purpose of the investigation.

4. **Handling of Footage:** Downloaded clips **must not** be moved, copied, or shared from the secure folder without explicit, documented authorisation from the RO, ensuring compliance with **UK GDPR** principles.

3. External CCTV Footage Requests (Data Subject Access & Legal)

External requests must be processed in strict compliance with the Data Protection Act 2018.

3.1. Subject Access Requests (SAR)

- **Definition:** An SAR is a request from an individual (or their legal representative/parent acting on behalf of the child) to view personal data of which they are the subject (including CCTV images).
- **Procedure:**
    - All SARs must be directed to the **Data Protection Lead (Claire Jones)** immediately.
    - The school must respond **within one calendar month** of receiving the request.
    - **Redaction Requirement:** The Responsible Officer must utilise **approved AI-powered redaction software** or an accredited **third-party redaction service** to obscure the identities (faces, identifiable features) of all third-party data subjects before releasing footage. Manual key-framing is only permitted in exceptional, low-risk circumstances and must be double-checked by the Deputy Responsible Officer.
- **Welsh Compliance Note:** Requesters may submit their request in Welsh. The school should be prepared to handle and respond to official data requests in the official language of the request, or provide clear guidance on the school's response language policy.

3.2. Requests from Law Enforcement

- **Police/Legal Authorities:** Footage requested by the Police (for crime prevention/detection) or other statutory bodies must be provided in line with the school's legal obligation and UK GDPR requirements.
- **Documentation:** The RO must **log all disclosures** of footage to external parties, including: the date, the requesting authority, the purpose of the request, and the specific footage disclosed.

4. System and Equipment Security

- **Secure Location:** The CCTV recording equipment (Digital Video Recorder/Network Video Recorder) is kept **securely locked** within the **Network Manager's Office**.
- **Physical Access:** Physical access to the Network Manager's Office is strictly controlled and limited to the Network Manager, the Responsible Officer, and other authorised IT personnel only.
- **System Security:** The CCTV system and all associated software are **password-protected** and subject to regular security updates to prevent unauthorised digital access.

5. Data Retention and Disposal

5.1. Retention Standard

- **General Rule:** All general CCTV footage (including downloaded clips unless required for a specific purpose) will be automatically overwritten and deleted after a maximum of **30 days**. This period is generally accepted by the **Information Commissioner's Office (ICO)** as proportionate.

5.2. Exceptions for Extended Retention

- Footage must only be retained beyond 30 days if it is required for a **legitimate and documented reason**, such as:
    - An **ongoing internal disciplinary or safeguarding investigation.**
    - **Legal reasons:** Required as evidence for a current or reasonably anticipated legal claim or proceedings.
- **Action Required:** Any decision to retain footage for longer than 30 days **must** be authorised in writing by the **Data Protection Lead** and documented in a retention log, clearly stating the legal basis for the extension.