Ysgol Gynradd Penderyn

SCHOOL CCTV POLICY V1.0

Document Information

Version:	Version 1.0
Status:	FINAL
Date:	March 2024

Mae'r ddogfen hon ar gael yn Gymraeg / This document is also available in Welsh

Contents

1. Introduction

The School is committed to respecting people's rights to privacy and supports the individual's entitlement to go about their lawful business. This is the primary consideration in the operation of any CCTV system operated by the school. We are committed to complying with our data protection obligations and to being concise, clear, and transparent about how we obtain and use Personal Information and how (and when) we delete that information once it is no longer required.

This Policy is intended to reflect the school's implementation of CCTV through following best practice advice from the Information Commissioner's Office (ICO). We will review and update this CCTV Policy regularly in accordance with our data protection obligations.
Any queries in relation to this Policy or any of the matters referred to in it should be submitted to the School's Responsible Officer at – **Ysgol Gynradd Penderyn.**

This Policy provides an overview of the school's governance arrangements in respect of use of CCTV. It includes organisational measures and individual responsibilities, which aim to ensure that the school complies with the CCTV Code of Practice and Data Protection legislation and respects the rights of individuals.

2. Scope

2.1 This Policy applies to all staff employed by the School, and to external organisations or individuals who operate CCTV systems on the School's behalf.

2.2 The Policy also applies to all Governors when representing the School.

2.3 This policy covers the purchase and use of CCTV equipment and the gathering, storage, use and disposal of visual image data.

2.4 This document should be read in conjunction with the School CCTV Handbook, CCTV systems Code of Practice and Operational Manual. Failure to comply with these documents could lead to disciplinary action, resulting in dismissal and potentially criminal proceedings against the individuals concerned.

3. Objectives of School CCTV systems

The primary purpose for which the School operates CCTV is crime prevention and detection (i.e. to detect, prevent, deter, and reduce crime). Schools also operate CCTV to:

- enhance the general security of the School, its building(s) and assets
- ensure the health and safety of employees, pupils, parents, and visitors to the school etc.
- safeguarding purposes
- to assist with complaints or concerns (i.e. CCTV images may be used as evidence to support an investigation into a complaint or concern)
- to assist with legal or insurance claims (i.e. CCTV images may be used as evidence to support or defend a claim)

3.1 It is important that everyone and especially those charged with operating the CCTV systems on behalf of the school understand exactly why each of the systems have been introduced and what the cameras will and will not be used for.

3.2 CCTV cameras will not be used to monitor the progress of staff or individuals in the ordinary course of their lawful business in the area under surveillance. Managers are not permitted to use the cameras to observe staff working practices, time keeping, or to assist them in the day-to-day management of their staff, without prior approval from HR and when carried out as part of an investigation and in accordance with the school disciplinary policy.

3.3 Individuals will only be monitored if there is reasonable cause to suspect a criminal offence or serious breach of discipline. Additionally, the observation for potential misconduct may only be committed when authorised by appropriate management and HR Officer where appropriate and in accordance with the school disciplinary policy.

4. Legislation

4.1 In addition to School policies, procedures, guidelines and Codes of Practice, CCTV and its operation are subject to legislation under:

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (DPA)
- Protection of Freedoms Act 2012
- BS 7958: 2015
- Information Commissioner's CCTV Code of Practice
- Regulation of the Investigatory Powers Act (RIPA)
- Human Rights Act
- Health & Safety at Work Act (HSW)
- Equal Opportunities Act
- Home Office Surveillance Camera Code of Practice
- Surveillance Camera Commissionaires Code of Practice

It will be rare for small CCTV systems to be required to respond to requests for assistance under RIPA, but Responsible Officers should contact the Council's CCTV Team whenever it occurs.

5. Governance

To ensure compliance with the CCTV Code of Practice and Data Protection legislation all staff must understand their roles and responsibilities when operating the CCTV system. This creates clear lines of leadership, accountability, and governance, as well as promoting a culture where personal information is valued and protected.

Headteacher

Overall accountability for CCTV rests with the Headteacher and the Governing Body.
It is also the responsibility of the Headteacher and Chair of Governors to designate a Responsible Officer (RO) for the CCTV system.
They must ensure that the Responsible Officer:

- is aware of their responsibilities relating to the control, management, and operation of the system.
- is adequately trained in the operation of the system (speak to your CCTV provider regarding this)
- is familiar with the legislation (e.g. GDPR), policies and procedures that underpin the use of the system and access to images
- knows how to handle requests for access to CCTV footage
- knows who to contact for further advice and guidance

Responsible Officer

The RO is responsible for the day-to-day control, management and operation of the system including dealing with requests for access to footage. Responsibilities may include but are not limited to:

- ensuring the CCTV system is operational (daily)
- ensuring the images captured by the system are clear and serve the purpose for which the CCTV is in operation (i.e. cameras are in focus, covering the right areas etc.)
- managing access controls for other employees (System operators) within the school that have access to the CCTV system (authorised users)
- maintaining a list of authorised users (including allocation of passwords to access the system)
- checking that appropriate signage is in place
- handling requests for access to and copies of footage
- acting as a first point of contact for enquiries relating to the use of CCTV
- authorising the release of data (footage).

- Ensuring all records are kept for annual CCTV audit report.

System Operators

In some circumstances other staff members may have access to the system. If this is the case:

- Staff operating CCTV systems are responsible for operating the equipment in accordance with requirements set out in current legislation, this policy document, School CCTV Handbook, CCTV systems Code of Practice and local Operational Manuals.
- They must ensure that their training is up to date.
- They maintain accurate records including –
    - Reason for accessing the system
    - Incident details
    - Date/Time of incident
    - Persons requesting
    - Result of search
    - Seeking authorisation from the RO before the release of footage
- They are responsible for bringing any faults or misuse of the equipment to the RO's attention immediately for repairs to be arranged and misuse investigated.

6. Data Protection Impact Assessments (DPIA)

6.1 If a school is considering installing a new CCTV system or changing the scope of an existing system (i.e. using it for a different purpose or significantly changing the locations of cameras and the areas they cover etc.), they should undertake a Data Protection Impact Assessment prior to procurement.

7. Purchase and deployment of CCTV cameras

7.1 It is crucial that serious consideration is given to the necessity for CCTV cameras in any given location, and to assess any impact of them on the privacy of individuals using the areas where cameras are to be installed.

7.2 Cameras are not to be installed in such a way that they can overlook private space such as inside private dwellings. Privacy zones must be set to ensure neighbouring properties / buildings are not included in the field of view.

7.3 Cameras and signs should be clearly visible.

7.4 Once authorisation is given to procure new or replacement CCTV cameras, advice should be sought from the Council's Procurement and CCTV teams to ensure that the correct procedures are followed.

7.5 It is a requirement under the Information Commissioner's Code of Practice and the National CCTV Strategy that any equipment purchased is fit for purpose and will meet the objectives set down for the scheme. There is also a clear requirement for all CCTV schemes to have an effective maintenance schedule and to be operated in accordance with the Code of Practice. Staff purchasing new CCTV equipment need to ensure these requirements are fully met.

7.6 The procurement of cameras that can be used for monitoring audio conversations or be used to talk to individuals are **prohibited,** as this is seen as an unnecessary invasion of their privacy.

7.7 Once any new cameras have been installed, a copy of a map or building plan showing the location of the CCTV cameras should be sent to the CCTV Team for inclusion in the central CCTV asset library.

8. Monitoring

8.1 The main recording equipment Networked Video Recorder (NVR), Digital Video Recorder (DVR) or servers and switches must be secure, password protected and held in a locked cabinet with restricted access.

8.2 Any CCTV visual displays should not be placed in areas which can be observed by pupils, public, other staff.

8.3 The RO must ensure that those observing the visual displays are properly trained in their duties and responsibilities and that the ability to view the display is restricted to only those authorised to see it.

8.4 The RO must delegate suitable staff to operate the system (Operators). Operators must have a sound knowledge of the system and complete a full Incident report whenever they use the system. Systems can be set so individuals use designated username and passwords to log in, RO's are responsible for and must maintain accurate records in preparation for annual audit.

9. Recorded images reviews and the provision of evidence

9.1 It is critical that a full and detailed record is kept of all recorded image reviews of the systems and all instances when video images are given to another person or agency. This information is subject to an annual audit and must include:

- Date, time, camera number and location of the incident.
- The name of the authorising officer,
- The date time, name and contact details of the person reviewing or removing images,
- The reason for the review/issue of images and
- The signatures of the individuals who released and the received the images,
- Any media containing images should be uniquely marked and the number recorded for ease of identification.

9.2 Reviews must only be undertaken for a specific, legitimate purpose. The casual review or trawling of recorded images by anyone is strictly forbidden (including using a mobile phone to take a screenshot).

9.3 The release of evidence or permission to view images can only be authorised by the RO, Headteacher or Chair of Governors, dependent on the circumstances.

9.4 Further guidance regarding the release of footage to internal or external requestors is available in the School CCTV Handbook.

10. Retention

10.1 Images are retained for a period of 31 days to comply with SCC guidelines.

10.2 In the event of a request for CCTV images the footage may be retained on a secure drive pending a formal request. This is to ensure the footage is not lost through technical issues or overwritten. Footage can only be deleted once the requesting party has taken control and responsibility of the clip/image.

11. Signage

11.1 All areas where CCTV is in use should be clearly signed to comply with the Data Protection Act. This is to warn people that they are about to enter an area monitored by CCTV cameras or to remind them that they are still in an area covered by CCTV. The signs will also act as an additional deterrent. CCTV signs should not be displayed in areas which do not have CCTV cameras.

11.2 The sign should carry the organisations logo and a suitable contact number for the system operator (RO). The signs, position and the message needs to be big enough to enable people to easily read the information on it. For pedestrians the sign should be A3 or A4 size and for vehicle access A3 size (see Appendix A for the sign graphic).

12. CCTV image recording systems

12.1 Except for evidential purposes, images will not be extracted or copied in whole or in part by any means (including using a mobile phone to take a screenshot) printed onto paper/emailed etc.

12.2 Recorded material will not be sold or used for commercial purposes or for the purposes of entertainment. Images provided to the Police or other enforcement agencies or for internal investigations shall at no time be used for anything other than the purposes for which they were originally released.

12.3 All images will remain the property and copyright of the School.

12.4 Each new recording media must be clearly marked with a unique reference number in indelible ink before it is brought into operation.

12.5 All media will be disposed of securely when no longer required.

12.6 Details of what software required to view or play footage must be provided to enable the police and other agencies to view evidence on their own systems. Requesting parties may need to download the software prior to viewing. The School's ICT support may need to support the download.

13. Disciplinary offences and security

13.1 Tampering with or misuse of cameras, monitoring or recording equipment, documents or recorded data by staff may be regarded as misconduct and could lead to disciplinary action, which may result in dismissal or criminal prosecution.

13.2 Any breach of this policy document or the CCTV Code of Practice will be regarded as a serious matter. Staff who are in breach of this instruction may be subject to action under the Rhondda Cynon Taff County Borough Council disciplinary procedures.

13.3 The responsibility for guaranteeing the security and proper use of the system will rest with the responsible officer of the system concerned. These officers will, in the first instance, investigate all breaches or allegations of breaches of security or misuse and will report his/her findings to their head of service and director.

14. Health and safety

14.1 The responsible officer is to ensure that staff are made aware of and comply with all School policies on health and safety. They are to be aware of policies relating to working with electrical equipment, VDU Regulations.

15. Complaints

15.1 Complaints about the operation of a CCTV system should be addressed initially to the RO. All complaints will be dealt with in accordance with School Third Party Complaints procedure.

16. Further advice / information

16.1 Further advice on CCTV related matters may be obtained from the individuals and organisations shown below (add names, telephone numbers and email addresses below each name):

- General advice from their own line managers
- Advice on CCTV issues from the Council's CCTV Team
- Legal Advice and RIPA from the Head of Legal Services
- Advice on issues affecting staff from the HR Department
- Third Party Access Requests from the Data Access Officer
- Health and Safety advice from Departmental H&S Advisor
- Technical advice and training on individual systems from Systems Installer and the Council's CCTV Team

Appendix A – An example of CCTV sign

Appendix B - Surveillance Camera Commission 12 guiding principles

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.