



GIG
CYMRU
NHS
WALES

Iechyd Cyhoeddus
Cymru
Public Health
Wales

Reference Number: AW16/TP05
Version Number: 1.0
Date of Next review: 08/12/2025

SURVEILLANCE CAMERA (CCTV) PROCEDURE

Aim and Objectives

Public Health Wales is committed to providing a safe and secure environment for all staff, users and visitors to its premises.

Where made available Surveillance Cameras ((SC) formally known as CCTV) will be used to view and record events, thereby protecting Public Health Wales staff, users and assets, preventing and deterring crime, and securing the successful prosecution of offenders.

The aim of this procedure to formulate consistent working practices in relation to the use of SC on Public Health Wales premises (owned leased or other agreement). These practices will help to ensure compliance with the relevant legislation and protect data held by Public Health Wales whilst allowing appropriate levels of access to material when requested by individuals or other agencies.

The objectives of the Procedure are to meet the documentary and other accountability requirements of data protection legislation by identifying:

- the legal basis under which Public Health Wales operate SC systems
- roles and responsibilities
- the approval process for a new SC installation
- the process for viewing / retrieving and disclosing images from SC systems
- training requirements
- data retention requirements.

Linked Policies, Procedures and Written Control Documents

[NHS Wales Information Governance Policy](#)
[DPIA - Surveillance Cameras \(CCTV\)](#)

Scope

This procedure and any arrangements made under it applies to:

- All persons employed or engaged by Public Health Wales, including part time workers, temporary and agency workers, those holding honorary contracts and those engaged by the NHS Wales Health Collaborative
- All service users, visitors and volunteers

Where Public Health Wales provides services with other organisations, including health boards, the policies and procedures of the employing

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| organisation including honorary contract holders will apply. Where appropriate joint working arrangements will be agreed and for shared premises a Service Level Agreement/Memorandum of Understanding or alternative agreement will be in place. | |
| Equality and Health Impact Assessment | This procedure is subject to the EHIA completed for the Information Governance Policy IG EHIA Policy |
| Approved by | Information Governance Group |
| Approval Date | 08/12/2022 |
| Review Date | 08/12/2025 |
| Date of Publication: | 11/01/2023 |
| Accountable Executive Director/Director | Rhiannon Beaumont-Wood, Executive Director Quality, Nursing and Allied Healthcare Professionals. |
| Author | Stephen Williams Information Governance Manager. |

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the [Corporate Governance](#).

| Summary of reviews/amendments | | | | |
|--------------------------------------|-----------------------|-------------------------|-----------------------|------------------------------|
| Version number | Date of Review | Date of Approval | Date published | Summary of Amendments |
| 1.0 | October 2020 | 08/12/2022 | 11/01/23 | First issue |

1. Introduction

Public Health Wales operates a surveillance system (“the system”) in a number of sites throughout Wales. This document sets out the appropriate actions and procedures, which must be followed to comply with the Data Protection Act in respect of the use of Surveillance Cameras managed by Public Health Wales and will include buildings subject to shared working arrangements.

Surveillance Camera (SC) system is the new portmanteau term for what used to be referred to as CCTV (closed circuit TV) that reflects changes in technology. It includes CCTV but also newer technologies such as Body Worn Cameras (BWC), Unmanned Aerial Systems (Drones), Facial Recognition, Surveillance in Vehicles and Action Cameras some of which including those that incorporate Artificial Intelligence (AI) ¹

The capturing of images, audio and video relating to individuals, be they staff or members of the public constitutes processing of personal data under data protection legislation. Public Health Wales will be a data controller for all data captured through its SC systems, and each separate system must have an identified legal basis for its existence and must comply with the principles of fair processing. This is achieved through the above mentioned comprehensive *Data Protection Impact Assessment (DPIA)*, which should be read in conjunction with this procedure and which identifies the key attributes and controls relating to each system and identifies the purposes for which the system is used and how long any recorded data is kept.

Where SC systems are the responsibility of Public Health Wales, all staff must abide by this procedure and comply with procedures detailed within it.

For the purposes of this procedure, the term images should be interpreted as meaning images, video and audio, both live and recorded.

¹ Surveillance Camera Systems are defined in section 26 of the Protection of Freedoms Act.

2. Purpose of Processing

Public Health Wales operates a number of SC systems across its estate for the purposes of

- the prevention and detection of crime and disorder
- the safety of staff and where appropriate service users
- the protection of public health

All local systems are required to have a statement of the need for the system and as indicated above this is included in the linked comprehensive *Data Protection Impact Assessment*.

3. Legislative framework

The main legislative requirements relating to the use of SC are the same that apply to the processing of other forms of personal data and are to be found in the General Data Protection Regulation 2016 and the Data Protection Act 2018. However, due regard has also been paid to the following:

- The Protection of Freedoms Act 2012
- The Human Rights Act 1998
- The Regulation of Investigatory Powers Act 2000
- The CCTV Code of Practice produced by the Information Commissioner
- The Surveillance Camera Code of Practice produced by the Surveillance Camera Commissioner (as amended) 2021
- Caldicott Report 1997

4. Legal Basis for Processing

As the data controller, Public Health Wales is required to establish the legal basis for processing under General Data Processing Regulation (GDPR) as incorporated into the Data Protection Act 2018. In almost all cases, the legal basis for processing will be Article 6(1)(f) – Legitimate Interests GDPR. SC systems will not be used for capturing special category data.

In the past some of the cameras have been used in connection with service delivery, such as spotting packages that are available for collection. Were this usage to be resumed the lawful basis for processing in that case would be Article 6(1)(e) – Establishment Order. This would also be the case were the cameras required to satisfy a statutory requirement such as the Mortuary Regulations.

The processing of video surveillance camera data is in all cases ancillary to and compatible with the performance of Public Health Wales tasks and duties.

Public Health Wales will ensure fair processing through its Privacy Notice, and also by ensuring that appropriate signage is provided at all sites where SC are installed.

5. Roles and responsibilities

The Head of Information Governance is responsible for:

- Maintaining a system and process for approving the installation of new SC systems
- Approving the installation of new SC systems in conjunction with the Head of Estates
- Maintaining this procedure and any associated guidance
- Maintaining the DPIA for Surveillance Cameras
- Vetting requests to access images on the systems and maintain a log of requests
- Identifying appropriate data protection training for operatives of SC equipment

The Head of Digital IT Services is responsible for

- Ensuring that the technical specification of the equipment is appropriate and adequate for the purposes identified in DPIA.
- Technical security such as the encryption of data.

The Head of Estates and Facilities is responsible for:

- Approving the installation of new SC systems in conjunction with the Head of Information Governance
- In liaison with the services located in the building identifying which staff will act as local leads and have operational responsibility for a set of cameras
- Any technical training of operatives on the operation of the equipment.

Local leads for premises are responsible for:

- Operational oversight including ensuring appropriate staffing is available to be trained and operate the equipment
- Sign-posting requests for access.

and in liaison with the Building Manager and the Head of Estates and Health & Safety:

- Ensuring that the positioning, field of view and acoustic pickup of the equipment are appropriate and do not encroach on any areas where there would be an expectation of privacy.
- Arranging for routine maintenance and servicing of the equipment and the rectification of faults

Directors are responsible for:

- ensuring that any Body Worn Cameras (BWC) and other mobile surveillance equipment including Surveillance in Vehicles and Action Cameras are notified to the Head of Information Governance and subject to the DPIA procedure.

All managers are responsible for:

- ensuring that any access to SC data by their service or by a member of their staff has been properly authorised.

6. Approval Process for new SC installations

- 6.1. No new SC system will be installed on any part of the Public Health Wales estate without prior written approval from the Head of Information Governance and the Head of Estates and Facilities.
- 6.2. Any proposed new installation will trigger a requirement for the Data Protection Impact Assessment to be amended and the person responsible for it must consult with the Head of Information Governance.
- 6.3. The person responsible for the new installation will complete the site survey questionnaire (which forms part of the DPIA process) to the satisfaction of the Head of Information Governance and the Head of Estates and Facilities before written approval is granted.

- 6.4. Similarly, no body worn cameras, vehicle-based systems or Go cameras should be operationalised until the relevant DPIA has been completed and approved by the Head of Information Governance.

7. Access to Surveillance Camera Data by Staff

- 7.1. The viewing of any images from a SC system is classed as processing of personal data in the same way that accessing or viewing a service user's health record is. Accordingly, no person will access any recording or live images of SC systems without proper authorisation.
- 7.2. Staff authorised to operate the SC system and their managers may view live and recorded images and data in connection with their SC duties.
- 7.3. Any member of staff requiring access to the images must advise their manager who will seek advice and approval from the Head of Information Governance by completing the form at Annex 1.

8. Requests for Access from data subjects and other agencies

- 8.1. Anyone receiving a request for access to images from a data subject (the person or people captured on the system), must notify the Head of Information Governance without delay. No images are to be released or viewed without approval from the Head of Information Governance.
- 8.2. Requests for access from external agencies such as the Police should be directed to the Head of Information Governance.
- 8.3. Authorised SC operatives and their managers may release images and data to the Police or security services where the matter is urgent and where the identity and status of the applicant has been verified, but will be required to document any access granted and forward details to the Head of Information Governance as soon as possible.
- 8.4. The Head of Information Governance will maintain a record of all requests for access whether internal or external and the outcome.

9. Information Retention

- 9.1. The Guidance on Record Retention & Destruction is that CCTV recordings shall be retained for 28 days and then erased permanently.
- 9.2. The DPIA survey and actions will aim to ensure that retention parameters are set accordingly where system capabilities allow.
- 9.3. Where images or other data are extracted any copies will be deleted once the purpose has been discharged.
- 9.4. Information used as a reference database for matching purposes will be accurate and kept up to date.

10. Monitoring and Review

- 10.1. This procedure will be reviewed at least every 3 years or earlier if legislation changes.

INTERNAL REQUEST TO ACCESS SURVEILLANCE CAMERA (CCTV) DATA



| | |
|-----------------------------------------------|--|
| Name of the person making the Request: | |
| Department: Position: | |
| Address: | |
| Telephone Number: | |
| Date of Request | |

DETAILS OF IMAGES TO BE VIEWED/DISCLOSED

| | |
|---------------------------------------------------|--|
| Date of recording: | |
| Description of Data to be viewed/ accessed | |
| Reason: | |

| | | | |
|------------------------|--|----------------------------|--|
| Name of Manager | | Position of Manager | |
|------------------------|--|----------------------------|--|