Llanelli Town Council

DRAFT CCTV POLICY

OCTOBER 2026

Contents

1. Introduction
2. Objectives
3. Legislation
4. Responsibilities
5. Purchasing and Deployment of CCTV Cameras
6. Monitoring
7. CCTV Checks and Assurance
8. Viewing footage
9. Signage
10. Storage and Retention
11. Advanced Surveillance Technologies
12. Inspections
13. Health and Safety
14. Compliance measurement
15. Custodian
16. Complaints
17. Version History

1. Introduction

1.1. This policy governs surveillance camera equipment and the collection, retention, usage, and disposal of data recorded by Closed-Circuit Television (CCTV) systems. The Council currently only implements a CCTV systems for licensing and police purposes, monitoring areas within the licensed area at the Selwyn Samuel Centre only. For the purposes of this policy, all such devices will be collectively referred to as 'CCTV systems'.

1.2. This policy aims to set out standards relating to the use of such equipment that maximises effectiveness whilst at the same time minimises interference with the privacy of individuals whose images are captured by the devices.

1.3. This policy applies to all overt CCTV systems operated by the Council;

1.4. Llanelli Town Council is referred to as 'the Council' throughout this policy.

1.5. This document should be read in conjunction with relevant codes of practice from both the Biometrics and Surveillance Camera Commissioner and the Information Commissioner’s Office.

1.6. This policy will be made available on the Council's website.

2. Objectives

2.1. It is important that everyone and especially those charged with operating the CCTV systems on behalf of the Council understand exactly why each of the CCTV systems and each camera used as part of a CCTV system has been introduced and what the cameras should and should not be used for.

2.2. Each CCTV system will have its own site or task specific objectives. These could include some or all the following:

- Protecting areas and premises used by council officers and the public.
- Deterring and detecting crime and anti-social behaviour.
- Assisting in the identification of and apprehension of offenders.
- Deterring violent or aggressive behaviour towards council officers.
- Protecting council property and assets.
- Assisting in grievances, formal complaints and investigations.
- Monitoring operational environments.

3. Legislation

3.1. CCTV systems are subject to legislation under:

- The Data Protection Act 2018 (DPA).
- UK General Data Protection Regulation (UK GDPR).
- The Human Rights Act 1998 (HRA).
- The Freedom of Information Act 2000 (FOIA).
- The Protection of Freedoms Act 2012.
- The Criminal Procedures and Investigations Act 1996.
- The Regulation of Investigatory Powers Act 2000 (RIPA).
- Computer Misuse Act 1990.
- The Health & Safety at Work Act 1974.

4. Responsibilities

4.1 The Senior Information Risk Owner (SIRO) – Town Clerk

4.1.1. The SIRO ensures the delivery of a corporate approach to the Council's responsibilities arising from Protection of Freedoms Act 2012. They have strategic responsibility for the integrity and efficacy of the processes in place, which ensure compliance and in respect of all surveillance cameras operated by the Council.

4.2 CCTV Single Point of Contact – Town Clerk

4.2.1. The CCTV Single Point of Contact (SPOC) is responsible for overseeing all aspects related to surveillance cameras. They ensure that everyone involved in the use of CCTV systems is informed about current legislation and guidance relating to these systems.

4.2.2. The overall responsibility for CCTV systems rests with the Town Clerk. This includes ensuring all relevant staff are appropriately trained and all systems are used in accordance with this policy.

4.2.3. The Town Clerk will nominate a designated Officer who will liaise with the CCTV Operators of the system.

4.3 CCTV Officer – Principal Officer

4.3.1. CCTV Officers will have oversight of all CCTV systems managed by the service and will be a central point of contact and offer advice in relation to queries from staff. They will be responsible for ensuring that Self Assessment Templates (SATs) are in place for all systems, that the corporate Data Protection Impact Assessments (DPIAs) cover all systems and that these documents are reviewed on an annual basis and available for publication.

4.3.2. CCTV officers will ensure that the necessary steps are taken before installing a new system or making changes to existing ones, including the completion of EOI and consultation.

4.3.3. The designated CCTV Officer is responsible for the daily operation of each CCTV system. This applies to third parties operating under the Council's direction.

4.3.4. The CCTV Officer shall ensure that council officers involved in the operation of the CCTV system are trained in the use of the equipment and are aware of this policy and the procedures in place to manage CCTV systems at the Council.

4.3.5. The CCTV Officer should act as the first point of contact for all enquiries relevant to the CCTV system and should ensure that only authorised council officers are able to operate or view images.

4.3.6. The CCTV Officer shall investigate any reported misuse of a CCTV system and report it immediately to the CCTV SPOC.

4.3.7. The CCTV Officer shall ensure the CCTV system is operational and take steps to deal with any faults as appropriate.

4.3.8. The CCTV Officers will ensure that the necessary steps are taken before installing a new system or making changes to existing ones, including the completion of the EOI and consultation.

4.4 CCTV Operators

4.4.1. Council officers operating CCTV systems must comply with current legislation, this policy, guidelines, codes of practice, and local manuals. They must know the UK GDPR and DPA requirements.

4.4.2. Council officers involved in the use of CCTV systems shall report any misuse to the CCTV Officer and shall cooperate with any investigation. The CCTV Officer shall report it immediately to the CCTV SPOC and investigate any reported misuse of a CCTV system.

4.4.3. Council officers operating CCTV systems shall be responsible for bringing any equipment faults to the CCTV Officer's attention immediately.

5. Purchasing and Deployment of CCTV Cameras

5.1. All new or significantly altered CCTV systems intended for use by the Council must receive formal sign-off from the Town Council or Delegated Committee, prior to implementation. This approval process must be in accordance with the Council's Financial Regulations.

5.2. Those responsible for introducing and operating CCTV systems must ensure that the use of cameras is proportionate to the intended objective and that individuals' right to privacy is always respected. A report must be provided to the Town Council or Delegated Committee with a clear operational objective for the CCTV system and the relevant DPIA checked to ensure it covers the system.

5.3. Care must be taken to ensure that cameras do not capture images or sounds of private spaces such as private houses.

6. Monitoring

6.1. CCTV monitors installed in public spaces are designed for live surveillance. The practicality of these installations should be assessed individually, considering the business and operational requirements, as well as determining the appropriate personnel and members of the public who can view the footage.

6.2. Accessing of recorded CCTV footage must only be carried out by persons authorised by the CCTV Officer.

6.3. CCTV footage must not be downloaded without an approval to disclosure being submitted and approved.

6.4. CCTV will only be subject to the UK GDPR if the footage captured "relates to living individuals who can be identified" from it.

6.5. If the UK GDPR applies, the CCTV operator will be required to carry out the following:

6.5.1. Put up signs notifying people that CCTV is in use (see section 9).

6.5.2. Give any individual who requests it copies of footage of themselves (Subject Access Request) in consultation with the Data Protection Officer (see 8.3).

6.5.3. Ensure that any footage stored is kept for no longer than necessary for the purposes for which it is obtained.

6.5.4. Ensure that footage is not disclosed to anyone unless it is permitted under an exemption contained under the Data Protection Act 2018 and UK GDPR.

6.6. In addition to the obligations under the Data Protection Act 2018, the Human Rights Act requires any public authority using CCTV cameras to do so compatibly with Article 8 of the convention.

6.7. Details of CCTV systems data collection are included in the Council's privacy notice for CCTV.

6.8. Remote access to CCTV systems must adhere to secure corporate protocols set by the Digital Services team. Requests must list users who will have access and be approved by the Head of Service and SIRO.

7. CCTV Checks and Assurance

7.1. CCTV Operators must carry out routine checks to ensure that all CCTV equipment is functioning correctly. These checks include regular (e.g. weekly) visual inspections of cameras, monitors, recording equipment and associated operating systems. Any faults, defects or performance issues identified must be reported immediately in line with local fault-reporting procedures.

7.2. CCTV Officers are responsible for undertaking periodic inspections of all CCTV systems within their remit to provide assurance that systems remain operational, fit for purpose and compliant with this policy. These inspections must be completed at least annually and must include reviewing operator check records, monitoring the resolution of reported faults, and identifying any areas of non-compliance. Any non-compliance identified must be reported the CCTV SPOC or the SIRO.

8. Viewing footage

8.1. CCTV footage viewing must be conducted solely for legitimate reasons, such as operational needs or surveillance and monitoring at a site to prevent crime or antisocial behaviour. The Council, along with the CCTV Officer, will define the use of the CCTV system on a site-by-site basis.

8.2. The casual viewing or trawling of footage is strictly forbidden. Viewings must only be carried out for a specific, legitimate purpose. Inappropriate access must be reported and may lead to disciplinary action.

8.3. Under Article 15 of the UK GDPR, data subjects have the right to access information held about them by the Council and to have a copy of that personal data. Individuals also have the right to access images of themselves recorded on CCTV systems controlled by the Council. Such requests must be made in writing to the Data Protection Officer, Llanelli Town Council, The Old Vicarage, Town Hall Square, Llanelli, SA15 3DD or dataprotection@llanellitowncouncil.gov.uk. Please see the Council website for further details.

8.4. In the event of a request being received by another officer, that officer should contact the Data Protection Officer to discuss the request.

8.5. On occasion, council services may wish to access images and recordings captured on CCTV systems as part of a legitimate investigation into criminal activities, civil claims, potential disciplinary matters, complaints, grievances or health and safety issues. Viewings and images will only be released to a properly authorised investigating council officer upon the submission of a formal request to the CCTV Officer. The viewing request should include:

- The name of the authorising officer.
- The name and contact details of the person viewing images.
- The reason for viewing the images.
- Police requests for footage generally fall within the exemption outlined in Schedule 2, Part 1, Paragraph 2 of the Data Protection Act 2018. Access is authorised for the purposes of preventing or detecting crime, or apprehending or prosecuting offenders.
- Viewing requests must be made in a timely manner as the retention period for most CCTV systems in operation in the Council is one month. Council officers who are subject to Council disciplinary, complaints or grievance procedures have the right to see and retain footage of themselves and can request copies as a Subject Access Request as outlined in 8.3.
- On occasion, police officers may request to view images taken from CCTV systems during the investigation of criminal activity. This is generally permitted under an exemption in the UK GDPR.
- Insurance companies and solicitors may request footage for personal injury or employers' liability claims, often due to car park damage disputes. As the footage may identify drivers or vehicles, it is considered personal information. Copies can be requested via a Subject Access Request to the Information and Data Protection Officer (see 8.3).
- A record of all disclosures is kept by the Data Protection Officer for a period of five years after administrative use is concluded. Details of any disclosures will also be recorded on the template held relating to the system which records all occasions when images are viewed.

9. Signage

9.1. All areas where fixed site CCTV is in use must be clearly signed. Such signs warn people that they are about to enter an area covered by a CCTV system or remind them that they are still in an area covered by a CCTV system. Signs will also act as an additional deterrent. CCTV system signs should not be displayed in areas that do not have CCTV cameras.

9.2. Signs must be an appropriate size depending on context.

9.3. Signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a CCTV system.

9.5. Corporate signage will be made available which will:

9.5.1. Be clearly visible and readable.

9.5.2. Confirm if the system is recorded or monitored or both.

9.5.3. State the purpose for having a surveillance system in place.

10. Storage and Retention

10.1. CCTV system footage is stored for 30 days and then overwritten.

10.2. Access to CCTV footage will be kept secure in accordance with the Council's information security policy.

10.3. All footage will be stored securely in accordance with the Council's information security policy.

10.4. Data Residency and International Transfers: All CCTV footage, including that captured by smart doorbell cameras, should be stored in data centres located within the United Kingdom or European Economic Area (EEA), or with cloud service providers who guarantee UK/EEA data residency and full compliance with UK GDPR.

10.5. Where footage is stored or processed outside the UK/EEA, the Council must ensure that appropriate safeguards are in place, such as Standard Contractual Clauses, and that the rights and freedoms of data subjects are protected to the same standard as required by UK GDPR.

10.6. The location of all CCTV data storage must be documented in the system register and reviewed as part of the Data Protection Impact Assessment (DPIA).

10.7. All footage remains the property and copyright of the Council.

10.8. All footage is time and date stamped.

10.9. All media and CCTV devices will be confidentially disposed of when no longer needed following the Council's disposal procedure.

10.10. Recorded material will not be sold or used for commercial purposes.

10.11. For further information, please see the Council's policy on Handling personal data.

11. Advanced Surveillance Technologies

11.1. The Council does not currently permit the use of AI-based analytics or facial recognition technologies within its CCTV systems. Any future deployment of such technologies must undergo a Data Protection Impact Assessment (DPIA), ethical review, and receive formal approval from the SIRO. This includes systems capable of biometric identification, behavioural analysis, or automated decision-making.

12. Inspections

12.1. Council owned CCTV systems can be inspected at any time by:

- The SIRO.
- The CCTV SPOC.
- The relevant CCTV Officer.
- A member of the relevant regulatory body.

13. Health and Safety

13.1. This policy should be read in conjunction with the Council's Health and Safety Policy.

14. Compliance measurement

14.1. Adherence to this policy is mandatory and will be subject to monitoring by the Town Council and delegated Committees. Any violations of this policy by staff may result in disciplinary measures.

15. Complaints

16.1. Any complaints regarding CCTV systems operated by the Council will be dealt with in accordance with the Council's Complaints Policy.

17. Version History

Version	Date	Actioned By	Revision Description	Approved By
Closed Circuit Television Policy	October 2026	Arfon Davies	Created new policy	