



St Asaph City Council

CCTV Policy

A Policy to regulate the use of CCTV

Legal Context

This policy aims to ensure that the Council complies with the following legislation and codes of practice:

- The Data Protection Act 1998,
- The Human Rights Act 1998,
- The Information Commissioner's Code of Practice for CCTV 2008.

The Purpose of this Policy

This policy is to control the management, operation, use and confidentiality of the CCTV systems at the location specified at the end of this document. It sets out to comply with best practice in the CCTV Code of Practice, Charter for a democratic use of video-surveillance and other relevant guidance.

1. Introduction

- 1.1 This policy is to control the management, operation, use and confidentiality of the CCTV system at the location specified at the end of this document.
- 1.2 This policy will be subject to annual review by the City Council to ensure that it continues to reflect the public interest and that it and the systems meet all legislative requirements, principally:
 - a) Data Protection Act 1998,
 - b) Human Rights Act 1998.
- 1.3 The Council also wishes to adopt best practice and protocols set out in national guidance, including:
 - a) The CCTV Code of Practice,
 - b) Charter for a democratic use of video-surveillance
- 1.4 This policy aims to ensure that the Council's CCTV installations:

- a) are correctly and efficiently installed and operated.
- b) The City Council accepts the principles of the 1998 Act based on the Data Protection Principles as follows:
 - i. Data must be fairly and lawfully processed;
 - ii. Processed for limited purposes and not in any manner incompatible with these purposes;
 - iii. adequate, relevant and not excessive;
 - iv. accurate;
 - v. not kept for longer than necessary;
 - vi. processed in accordance with individuals' rights;
 - vii. secure;
 - viii. not transferred to countries with inadequate protection;
 - ix. subject to guidance on good practice;
 - x. data will not be used for personal gain or interest.

2. Statement of Purpose

2.1 To provide a safe and secure environment for the benefit of those who might visit, work or live in the vicinity of the premises. The system will not be used to invade the privacy of any individuals, except when carried out in accordance with the law.

2.2 The scheme will be used for the following purposes:

- a) to reduce the fear of crime by persons using the City Council amenities so they can enter and leave without fear of intimidation by individuals or groups;
- b) to reduce the vandalism of property and to prevent, deter and detect crime and disorder;
- c) to assist the Police, the City Council and other Law Enforcement Agencies with identification, detection, apprehension and prosecution of offenders by examining and using retrievable evidence relating to crime, public order or contravention of bye-laws;
- d) to deter potential offenders by publicly displaying the existence of CCTV, having cameras clearly sited that are not hidden and signs on display;
- e) to assist all emergency services to carry out their lawful duties.

3. Location:

The Community and Council Meeting Room, Roe Plas Meadow, off High Street, St Asaph, LL17 0RF.

4. Management of the System

4.1 The CCTV operating system will be administered and managed by the Clerk of the Council in accordance with the principles and objectives expressed in this policy document.

- 4.2 All cameras are monitored on the site where they operate.
- 4.3 The CCTV system will be operated 24 hours a day, 365 days of the year.
- 4.4 Warning signs, as required by the Code of Practice of the Information Commissioner, will be placed at each side of the building covered by the Council's CCTV cameras.

5. System Control – Monitoring Procedures

- 5.1 Access to the CCTV system will be strictly limited to the Clerk, elected members of the Council and other authorised persons, such as Police Officers.
- 5.2 Unauthorised persons are not permitted to view live or pre-recorded footage.
- 5.3 The CCTV control room at the Meeting Room shall be kept locked at all times when not in use.
- 5.4 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.
- 5.5 Recording is carried out on digital data apparatus. These are located within the CCTV control room at the Meeting Room.

6. Retention and Disposal of Material

- 6.1 Data will be retained for 28 days before it is automatically overwritten.
- 6.2 USB devices containing material downloaded from the recorders will be disposed of by a secure method.
- 6.3 Footage will only be stored on USB devices if footage is requested by external agencies in the process of detecting crime and the prosecution of offenders.
- 6.4 In order to maintain and preserve the integrity of the data, USB devices used to record events from the CCTV cameras and the facility to use them in any future proceedings, the following procedures for their use and retention of data must be strictly adhered to:
 - a) Each USB device must be kept in a secure location with access restricted to the Clerk and members of the Council.
 - b) Data required for evidential purposes must be recorded as a pair, both bearing the same reference number. The Master Copy is to be kept by the City Council and the second copy can be released to the Police or other authorised third party on production of a signed data access request form.
 - c) Identical information should be loaded on both the Master and Copy USB devices.

- d) The Master USB device should be kept in a secure metal box. The Copy USB device is handed to the person making the request on production of positive ID such as Police Warrant Card, Picture ID Card, Driving Licence etc.
- e) The record sheet should then be completed and the Copy USB device signed for and counter-signed by the Clerk.

7. Dealing with Official Requests: use of CCTV in relation to criminal investigations

- 7.1 CCTV recorded images may be viewed by the Police for the prevention and detection of crime, authorised officers and members of St Asaph City Council for authorisation and training.
- 7.2 A record will be maintained of the release of the Data on USB device to the Police or other authorised applicants. A register will be available for this purpose.
- 7.3 Viewing of CCTV images by the Police must be recorded in writing and entered in the log book. This will be under the management of the Clerk. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.
- 7.4 Should a USB device be required as evidence, a copy may be released to the Police under the procedures described in this Policy. USB devices will only be released to the Police on the clear understanding that the USB device remains the property of the Council, and both the USB device and the information contained on it are to be treated in accordance with this policy.
- 7.5 The Council retains the right to refuse permission for the Police to pass to any other person the USB device or any part of the information contained therein.
- 7.6 The Police may require the Council to retain the stored USB device(s) for possible use as evidence in the future. Such USB device(s) will be properly indexed and stored under the management of the Clerk until they are needed by the Police.
- 7.7 Data may be released to the Council's insurers if required, as evidence of a claim or loss.

8. Complaints

- 8.1 Any complaints about the City Council's CCTV should be addressed to the St Asaph City Clerk.
- 8.2 Complaints will be investigated in accordance with section 5 of this policy.

9. **Access by the Data Subject**

9.1 The Data Protection Act provides Data Subjects (individuals to whom “personal data” relate) with a right to access all data held about themselves, including that obtained by CCTV.

9.2 Requests for information, including Data Subject Access Requests should be sent to:

Mrs Jill Ellison
City Clerk
St Asaph City Council
26 Maes Dolfor
Llanfairfechan
Conwy LL33 0RP

e-mail: clerk@stasaphcitycouncil.gov.uk

9.3 The Council may charge a fee of up to £10 for providing this information. The applicant must provide details that allow us to identify them as the subject of the information i.e. the date time and location.