WEST LOTHIAN COUNCIL
CCTV POLICY

Data Label: Public

CONTENTS

1. INTRODUCTION

West Lothian Council uses Closed-Circuit Television (CCTV) and surveillance systems to prevent and detect crime, to aid in public safety, to monitor council buildings and assets in order to provide a safe and secure environment for staff, volunteers, contractors, visitors and the public.

This policy applies to systems where West Lothian Council are Data Controllers. Operation of CCTV systems is covered by data protection law, including, the Data Protection Act 2018 and UK GDPR. The council is the Data Controller for the images produced by the CCTV systems it owns and are registered with the Information Commissioner's Office, Registration reference number Z6925127. Their use may be subject to the controls and procedures required by the Regulation of Investigatory Powers (Scotland) Act 2000.

This policy applies to CCTV and other surveillance camera devices that view or record individuals, and covers other information that relates to individuals, such as, vehicle registration marks.

This policy uses the term 'CCTV' and 'CCTV systems' throughout for ease of reference, that include (but are not limited to) the following types of systems:

- Fixed CCTV (networked);
- Body Worn Cameras;
- Automatic Number Plate Recognition (ANPR);
- Unmanned aerial systems (drones);
- Stand-alone cameras;
- Re-deployable/mobile cameras.

The Head of Corporate Services, in consultation with the Senior Information Risk Owner (SIRO), is authorised to adjust the wording of this policy where those changes do not represent any meaningful change to the policy. Meaningful changes require committee or council approval.

2. SCOPE

This policy applies to all CCTV and related surveillance systems where West Lothian Council are the Data Controllers.

Where a system is jointly owned or jointly operated, the governance and accountability arrangements are agreed between the partners and documented.

This policy is applicable to, and must be followed by, all staff including consultants and contractors and volunteers.

Elected Members are subject to the same rules that apply to employees when acting as a member of committee or personally in relation to information controlled or processed by the council and when the rights of data subjects in relation to that information apply. Elected members are data controllers under GDPR and are responsible for the personal data that they collect, store, use and delete.

When acting on behalf of a member of the public, Elected Members are entitled to have access to information held by the council where it is reasonably required for them to perform their councillor duties. Requests for personal data will be dealt with by officers under the relevant regulations and ICO guidance on the provision of personal data to elected representatives and the council's Officer/Member Protocol. That may require the authorisation by the data subject.

Covert surveillance is out with the scope of this policy. The use of covert cameras or recording / monitoring will be undertaken, in accordance with the council's Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) Policy.

3. RESPONSIBILITIES

3.1 Heads of Service

Heads of Service are ultimately responsible for ensuring that that the use of CCTV systems adhere to this policy and associated procedures. They will also assess the necessity for CCTV systems and address the balance between the necessity of the system and the privacy rights of individuals.

3.2 Property Services

Property Services are responsible for the technical aspects of CCTV systems, guidelines and procedures within the council, ensuring that all installations are recorded and managed in accordance with this policy. In addition, the Property Services Manager will:

- Provide advice and guidance on all technical CCTV related matters;
- Maintain a central register of all CCTV installations;
- Review existing CCTV systems on a regular basis to ensure that they continue to meet the technical compliance requirements and the principles of this policy;
- Update all users on technical changes to policy and associated procedures;
- Act as an advisor for technical enquires.

3.3 Service Manager/ Head Teachers

Service Managers are named individuals who are in control of the system and security of the CCTV equipment. This may include Control Room Managers, Head Teachers and/ or System Supervisors. The Service Manager will:

- Ensure the service completes a Data Protection Impact Assessment (DPIA) that covers the CCTV systems under their control;
- Assign a sufficient number of CCTV Operators for each system;
- Approves staff members to have operational access to CCTV equipment and recordings.
- Restrict access to recordings to only authorised staff;
- Ensure that authorised staff are appropriately trained in the application of this policy and associated procedures;
- Establish back up, retention, destruction and maintenance operations;
- Manage service CCTV complaints and requests for access to recordings;
- Maintain the security of CCTV Systems.

3.4 System Operators

Operators and other approved staff members are responsible for following procedures established for its use.

4. PRINCIPLES

4.1 The council only use CCTV for specified, legitimate purposes;

Each CCTV system has its own site or task specific objectives. These include some or all of the following:

- To assist the council in their enforcement and regulatory functions;
- Protecting property and assets used by council staff and the public;
- Deterring, detecting and recording crime and anti-social behaviour;
- Assisting in the identification of offenders leading to appropriate action/sanction;
- Reducing violent or aggressive behaviour towards staff and others working for the council;
- Assisting with staff disciplinary, grievance, formal complaints and Health and Safety Investigations.

The equipment utilised produces images that are of suitable quality to meet the specified purpose(s) for which they are installed. Equipment is regularly checked to ensure that the images remain fit for purpose, and that any date and time stamp recorded on the images is accurate.

4.2 Effects of CCTV on individuals and their privacy rights is assessed

Prior to implementing a CCTV system, the council will establish a legitimate purpose(s) for it and assess the balance between the necessity of the system and the privacy rights of individuals. All risks to the rights and freedoms of individuals are assessed in Data Protection Impact Assessments (DPIAs).

4.3 The council is transparent about its use of CCTV

CCTV systems are operated with due regard to the principle that everyone has the right to respect for his or her private and family life and home. The location of equipment is carefully considered and, kept under review, to ensure the system is effective while minimising intrusion and impact on individuals.

Unless the use of authorised under the council's Policy, Procedure and Guidance in relation to the Regulation of Investigatory Powers (Scotland) Act 2000, the presence of a CCTV system, the purpose for it and contact details for the council as Data Controller of it are clearly displayed to the public in signs and privacy notices.

4.4 Responsibilities for each CCTV system are recorded

Property Services keeps a register of all CCTV systems in operation and details of responsible parties for each. Responsibilities and accountability are also further defined in this policy and are recorded in DPIAs.

4.5 Procedures are in place and these are appropriately communicated

The council has in place CCTV procedures that provide operational guidance on the use of CCTV systems. Where appropriate, these are supplemented by localised procedures that govern individual installations.

These are accessible to all staff that handle and manage CCTV systems and recordings. Staff who have access to the system receive training and support to understand their role and responsibilities under this policy and associated regulatory framework.

4.6 Images are only retained for as long as required

Images will be retained for no longer than 30 calendar days unless required longer for evidentiary purposes, the investigation of an offence, or for any other lawful reason.

When images are no longer required they are overwritten or securely destroyed.

Images retained for evidential purposes are reviewed on a regular basis to ensure that disposals are carried out when required to do so.

4.7 Access to and disclosure of recordings is restricted

Access to recordings and any copies are restricted to only authorised personnel. The casual review or trawling of recorded images by anyone is strictly forbidden.

Viewing of recorded images out with daily monitoring must take place in a restricted area.

Further information on disclosures of recordings are detailed in section 5 below.

4.8 Operators are appropriately trained

Service Managers, operators and those authorised to access recordings will be appropriately trained and competent in the operational and technical standards for the handling and management of recordings and equipment. Training is refreshed on a regular basis.

4.9 Recordings are appropriately secured

Access to surveillance camera controls and monitors and to the servers and media containing surveillance images is appropriately secured through encryption of devices and media, firewall protection of the servers, user account access controls and physical security for the control area. Systems are secured against hardware attack and backed up appropriately. Where available, camera equipment and/or images are encrypted.

4.10 Systems are regularly audited

All CCTV Systems are subject to regular audits to ensure that they continue to remain fit for purpose, are still required for the purposes that they were installed, that they remain compliant with legislative requirements, with this policy and associated procedures.

4.11 Systems are used in the most effective way when required as evidence

The council only install and utilise CCTV Systems where it is deemed to be the most appropriate methodology. The council ensure safeguards are in place to ensure evidential value and integrity where required for public safety or law enforcement purposes.

4.12 Information used in data matching is kept accurate and up to date

The council do not match data captured on CCTV Systems.

5. REQUESTS FOR ACCESS/DISCLOSURE OF CCTV

CCTV recordings are held only by the council unless there is a legitimate reason to disclose them. Disclosure includes the viewing of images by someone who is not the service manager operator of the system or other approved staff member.

Recordings are only disclosed where there is a valid, legitimate reason, including:

- To the police, for the prevention and detection of crime;
- To a court for legal proceedings;
- To a solicitor for legal proceedings.

Where recordings have been disclosed or viewed by an authorised third party the council will keep a record of:

- When the images were disclosed;
- Why they have been disclosed;
- Any crime incident number to which they refer, where appropriate;
- Who the images have been viewed by or disclosed to.

5.1 Subject Access Requests

Individuals, or their appointed representative, may be granted access to recorded images of themselves by making a 'Subject Access Request'.

Where the Council is unable to comply with a Subject Access Request, the council will write to the individual advising them of the council's decision with explanation of the reasons for the refusal and any exemptions applied.

5.2 Requests by Third Parties

In limited circumstances, it may be appropriate to disclose images to a third party, such as, when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies. The council may also receive requests to disclose information in response to emergency circumstances, such as, danger to life.

All disclosures are made at the discretion of the council, with reference made to relevant legislation. Before disclosing any footage, consideration is given to whether (if possible) images of third parties should be obscured to prevent unnecessary disclosure. All requests are appropriately logged including details of the date of disclosure, recipient and reason for disclosure.

6. POLICY MONITORING AND REPORTING

Governance over this policy is built into normal council processes, e.g. line management, service management and project management. Formal governance over this policy is monitored and reviewed under the Information Governance Policy reporting arrangement.

7. OTHER RELEVANT POLICIES

Information Governance Policy

Special Category Data Policy

Policy, Procedure and Guidance in relation to the Regulation of Investigatory Powers (Scotland) Act 2000

8. REVIEW

This policy will be reviewed as appropriate at least once every 5 years. The Head of Corporate Services may make minor and administrative changes when required, for example, to reflect internal council management structure changes, or new legislation or guidance.

9. APPENDIX 1: DEFINITIONS

Audit - In the context of this policy, the service reviews various aspects of CCTV usage, including signage, data retention, access controls, and data protection impact assessments ensuring compliance with data protection regulations.

CCTV Systems - In the context of this policy, CCTV Systems is defined as any system used to monitor or record the activities of individuals or both in video and/or audio format. These include Closed Circuity Television systems, portable/mobile/re-deployable cameras, drones, Automatic Number Plate Recognition systems (ANPR) etc.

Covert Surveillance - Covert surveillance is the use of hidden cameras or equipment to observe and/or record the activities of a subject which is carried out without their knowledge.

Data Controller - The Data Controller is a legal person or organisation, which, alone or jointly with others, determines the purpose and manner by which personal data is processed. West Lothian Council are data controllers for CCTV systems covered by this policy.

Data Protection Impact Assessment (DPIA) - This is a process that helps to identify and minimise data protection risks. More information on DPIAs can be found on the ICO Web Site.

Data Protection Law - Data Protection Law includes the General Data Protection Regulation 2016/679; the UK Data Protection Act 2018, UK GDPR and all relevant EU and UK Data Protection legislation.

Staff - All council employees and workers, such as, contractors, consultants, volunteers and agency staff that have authorised access to council information/systems or process council information.

Technical Guidance - provision of information relating to camera type, placement, recording, signage, commissioning and maintenance.