WELLS CITY COUNCIL
CCTV POLICY

November 2025

Lisa Wassell
fm@wells.gov.uk

1. Introduction

This policy has been written in conjunction with Wells City Council's CCTV Code of Practice. It outlines the policies aim and objectives of the management of the Council's CCTV system.

2. Policy Statement

This policy outlines the organisations approach to the use of CCTV systems to ensure the compliance with legal obligations, protect privacy rights, and support the safety and security of staff, visitors and property.

3. Scope

This policy applies to all CCTV systems operation by Wells City Council , including fixed mobile cameras, and covers live monitoring, recording, storage, access and disclosure of footage.

4. Legal Framework

This policy complies with:

- The Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- The Surveillance Camera Code of Practice
- Human Rights Act 1998 (Article 8 – Right to Privacy)
- Protection of Freedoms Act 2012

5. Objectives

- To deter and detect crime, vandalism and anti social behaviour
- To enhance the safety of staff, visitors and the public
- To monitor operational activities to ensure compliance with health and safety
- To assist in investigations and legal proceedings when necessary

5. System Operation

- Cameras are positioned to monitor public areas, entrances, exits, car parks and key operational zones
- Cameras will not be used to monitor private areas such as toilets or break rooms
- Signage is displayed to inform individuals of CCTV usage in accordance with ICO guidelines

6. Live Viewing

- Designated staff may access live CCTV feeds for operational monitoring and incident response
- Live viewing is permitted only for legitimate business purposes and must not be misused
- Staff must be trained in responsible use and data protection principles
- Only trained and authorised employees of the Council are permitted to live view, monitors are not permitted to be in full of the public at any time.

7. Access to Recorded Footage

- Only designated and trained personnel may access recorded footage.
- All access must be logged using the CCTV Access Log
- Each review must be documented, recording:
    - Date and time
    - Purpose of review
    - Reviewer's identity and role
- Reviews must be for legitimate, documented reasons such as crime investigation or safety concerns.
- Footage will only be accessed for incident investigation, legal compliance, or safeguarding
- Disclosure to third parties (e.g. police) must be authorised by the Town Clerk and documented
- Access to recorded footage is only permitted by authorised devices, this being via the designated control box(s).

8. Training and Competency

- CCTV users must complete initial and annual refresher training.
- Training topics include:
- Legal obligations (GDPR, Data Protection Act)
- Ethical surveillance practices
- Technical system use and incident management

9. Data Retention

- Recorded footage will be retained for a maximum of 30 days, unless required for investigation
- Systems are configured for automated deletion after retention period.

- Stored footage is protected by access controls and encryption measures.

10. Dissemination and Disclosure

Disclosures are permitted only:

- To law enforcement agencies with lawful authority.
- Under subject access requests by individuals (UK GDPR Article 15).
- Through lawful court proceedings or legal representation.

All disclosures must:

- Be authorised by the Data Protection Officer.
- Be logged with recipient details, purpose, and footage description.
- Be redacted where necessary (e.g. blurring third-party individuals).

11. Public Awareness and Signage

- Clearly visible signs are located at entry points of the buildings to indicate surveillance.

12. Compliance, Audit, and Breach Reporting

- CCTV systems are password protected, and access is role-based
- Regular audits will be conducted to ensure compliance and detect misuse
- Any misuse or data breach must be immediately reported to the Data Protection Officer.
- Investigations will follow Council disciplinary protocols and safeguarding procedures.

13. Review and Updates

This policy will be reviewed annually or following significant changes in legislation, operations, or technology.

12. Contact

For questions or concerns regarding this policy, contact:

Data Protection Officer: Haylee Wilkins