CLOSED CIRCUIT TELEVISION (CCTV) POLICY

1. Purpose

The purpose of this policy is to regulate the management, operation and use of Closed Circuit Television (CCTV) systems operated by Yalding Parish Council ("The Council"). CCTV is installed to enhance the security and safety of residents, visitors, Members, Council property, and those passing through The Parish.

2. Scope

This policy applies to the location, operation, monitoring, recording, storage and use of CCTV images captured by systems owned by The Council.
The Council complies with the Information Commissioner's Office (ICO) Video Surveillance Guidance and the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).
Recognisable images captured by CCTV constitute personal data and will be handled accordingly. Prominent signage is displayed in all areas covered by CCTV. While the system is designed to maximise effectiveness, it cannot guarantee coverage of every incident. CCTV monitoring will be conducted in a manner consistent with all Council policies, including the Equality & Diversity Policy. Monitoring based on protected characteristics (e.g. race, gender, disability, sexual orientation, religion, or age) is strictly prohibited. CCTV will only be used in public areas where individuals have no reasonable expectation of privacy.

3. System Overview

CCTV is currently in operation:

- At The High Street, Yalding
- At The Lees picnic area and car park

Exclusion

The Council owns the CCTV camera located on Yalding High Street, but it was installed by Kent Police. At this time, The Council is responsible for maintenance only. The Council currently does not have access to the live feed or recorded images. Kent Police (Maidstone)

hold exclusive access and act as the Data Controller for that system. This camera is therefore excluded from this policy except to confirm its existence.

4. Data Protection Statement

The Council is the Data Controller for CCTV systems located at The Lees picnic area and car park. CCTV is installed for the safety and wellbeing of residents, visitors, and those passing through the parish. Access to stored images is strictly controlled. Use of images, including disclosure to third parties, will be in accordance with The Council's data protection registration. Signage is displayed stating the presence of CCTV and providing contact details for enquiries during office hours. Any introduction of new CCTV devices, relocation of existing cameras, or removal of equipment must be approved by The Council at a full Council meeting.

5. Intended Purposes of CCTV

CCTV surveillance is used for the following purposes:

- Promoting the health and safety of members, staff, and visitors
- Reducing crime and anti-social behaviour, including theft and vandalism
- Supporting the police in deterring and detecting crime
- Assisting in identifying, apprehending, and prosecuting offenders
- Ensuring that Council rules are respected

The system does not record audio. The CCTV system is owned and operated by The Council and deployment is determined by Council Members. All authorised operators are trained in the procedures for accessing and handling recorded images and are aware of their responsibilities under this policy and The ICO Video Surveillance Guidance. For the purposes of this policy, authorised operators are the individuals listed in Section 6.

6. Authorised Access

Yalding Parish Council is the Data Controller. Access to CCTV recordings is restricted to the following authorised personnel acting on behalf of the Council:

- The Clerk
- The Deputy Clerk
- Car Park Manager (as an authorised contracted operator)

The Car Park Manager, as a contracted operator acting on behalf of the Council, is authorised to access and operate the CCTV system strictly in accordance with this policy, the Council's Data Protection Impact Assessment (DPIA), and all relevant data protection legislation. As a condition of their contract, the Car Park Manager is required to comply fully with this policy, maintain confidentiality, and follow all procedures relating to the secure handling, access, logging, and disclosure of CCTV footage.

These individuals may access, view, retrieve and disclose CCTV images strictly in accordance with this policy and only for lawful purposes. No other Councillors, staff, or third parties may access CCTV images unless formally authorised by a resolution of The Council. The system is password protected, the password will be changed at least annually, and immediately if an authorised operator leaves or compromise is suspected.

7. Retention of Images

Recordings are stored on a secure hard drive and retained for 31 days, after which they are automatically overwritten unless required for the investigation of a specific incident.
Where cameras use a memory card that does not overwrite automatically, the card will be removed and securely stored for the 31 day retention period. If no incident has been reported during that period, the card will be securely wiped without the need to review the footage.
Where footage is retained for an incident, it will be securely stored only for as long as necessary to fulfil the purpose for which it was retained, including any legal or insurance processes. Once no longer required, it will be securely deleted.
The cameras do not have automatic power backup capability in the event of a mains failure.

8. Access to Images

Access and disclosure will be made only in accordance with the lawful bases set out in Article 6 of the UK GDPR, typically for preventing or detecting crime or complying with a legal obligation. Access is restricted and carefully controlled to protect individuals' rights and to maintain the chain of evidence. The Council may refuse to examine footage for minor or trivial events, where dates/times cannot be provided, or where the likelihood of the incident being captured is low.

9. Documentation of Viewing

Whenever images are accessed or viewed, copied or disclosed the following must be recorded:

- Name and role of the person authorising access
- Name of the person accessing or removing the recordings
- Date and time of access or removal
- Names and organisations of any persons viewing the images
- Reason for viewing
- Outcome of the viewing
- Date and time of return to secure storage

All access, viewing, copying or disclosure must be logged as soon as reasonably practicable, normally within office hours, but in any case within 72 hours of the access taking place.

10. Removal of Images for Legal Proceedings

Where recordings are removed for legal purposes, the following must be documented:

- Name of the person removing the recordings
- Date and time of removal
- Reason for removal
- Specific authorisation for removal and disclosure
- Any relevant crime or incident number
- Destination of the recordings
- Signature of the collecting police officer (where applicable)
- Date and time of return to secure storage

Routine automatic deletion after the 31 day retention period does not need to be logged. Routine 31 day memory card replacement and wiping does not require logging unless footage is accessed, viewed, exported, or retained for an incident.

11. Access by Third Parties

Requests for access must be made using the CCTV Access Request Form available on The Council's website. Disclosure will only be made in limited circumstances, including:

- Police, MBC/KCC Enforcement Officers and other statutory bodies
- Prosecution agencies
- Relevant legal representatives
- The media, where public assistance is required to identify a victim, witness, or suspect (taking into account the wishes of any victim)
- Individuals whose images have been recorded, unless disclosure would prejudice criminal enquiries

All requests and decisions must be documented. If access is denied, the reason must be recorded.

12. Access by Data Subjects

Individuals may request access to images of themselves under the UK GDPR and DPA 2018. Requests must:

- Be made using the CCTV Access Request Form
- Include sufficient information to identify the requester in the footage (date, time, description, proof of identity)

Footage may be edited to protect the identities of others.

The Clerk will:

- Locate the relevant images
- Determine whether third party images must be blurred
- Seek advice from the Council's insurers where appropriate

The Clerk will provide a written response within one calendar month of receiving the request, in accordance with UK GDPR. Where a request is complex or involves multiple requests, the Council may extend the response period by up to a further two months. If an extension is required, the requester will be informed within the initial one month period, together with the reasons for the extension

A copy of the request and response will be retained.

13. Editing and Blurring of Images

Third party images must be disguised or blurred where disclosure would reveal the identity of individuals who are not the subject of the request. This includes, but is not limited to:

- Footage released to a data subject where other individuals appear
- Footage disclosed to the media

- Footage provided to third parties where disclosure of other individuals would be inappropriate or unlawful

If the Council's CCTV system cannot carry out this editing, an external editing company may be used. In such cases:

- A written contract must be in place
- The company must provide appropriate security guarantees
- The company may only process images in accordance with the Council's instructions

14. Complaints

Complaints must be submitted in writing to The Clerk. Where the complaint relates to another individual, written consent from the data subject is required. Complaints will be acknowledged within 5 working days and responded to within 20 working days. If the complainant remains dissatisfied, they may escalate the matter to the ICO.

Adopted 07.04.2026

To be reviewed annually at the Annual Parish Council Meeting (see minutes of that meeting).