DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Close Circuit Television (CCTV) – The Lees Picnic Area and Car Park

1. Why a DPIA is required

A DPIA is required because the CCTV involves:

- Systematic monitoring of a publicly accessible area
- Processing of personal data of members of the public
- Potential disclosure to law enforcement and other agencies

This meets Information Commissioners' Office (ICO)'s criteria for requiring a DPIA.

2. Status of the deployment

- This DPIA relates to the existing CCTV at The Lees picnic area and car park.
- The Cameras are basic, off-the-shelf fixed CCTV units with no audio, no analytics, and no remote access.
- The Council processes data under the UK General Data Protection Regulations (UK GDPR) and Data Protection Act (DPA) 2018.
- The CCTV camera on Yalding High Street is owned by Yalding Parish Council (YPC) but controlled by Kent Police, who act as the Data Controller. It is excluded from this DPIA.

3. Purpose of the CCTV

The CCTV system is installed to:

- Promote the safety of residents and visitors
- Deter anti-social behaviour and low level crime
- support police investigations when incidents occur
- Protect Council property

Crime levels are generally low, but the CCTV acts as a preventative measure and provides reassurance to the community.

4. Whose data is processed and over what area

- Members of the public using or passing through The Lees car park

- Vehicles entering or leaving the area
- No audio is recorded
- No special category data is intentionally captured
- Children and vulnerable adults may appear incidentally
- Footage is retained for 31 days unless required for an incident

5. Decision-makers and data sharing

Data Controller: Yalding Parish Council

Authorised Operators: Clerk, Deputy Clerk and Car Park Manager

- Footage may be shared with:
- Kent Police
- Other statutory enforcement bodies
- Insurers
- Legal representatives
- Individuals requesting their own personal data

All disclosures follow the Council's CCTV Policy and are logged. 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.

6. Technology used

- 5 Fixed, stand-alone CCTV cameras
- No audio
- No ANPR
- No facial recognition
- No analytics
- No remote access
- Recording stored on a local hard drive or memory card

7. Information flow

- Cameras record continuously (24/7).
- Footage is stored on a secure hard drive or memory card.
- Footage is accessed only by authorised personnel.
- If relevant footage is found, it may be:
  - Viewed on site
  - Exported to a USB/memory stick
  - Disclosed to authorised agencies

8. Routine retention

- Hard drive footage overwrites automatically after 31 days and or
- Memory cards are swapped every 31 days and wiped
- Routine wiping does not require logging

9. Footage retained for incidents is securely stored until no longer required.

No live monitoring, no watchlists, no automated processing.

10. Recording capability

- Recording is enabled
- Recording takes place on site
- No audio recording

11. Disclosure method

- Footage exported to encrypted USB/memory stick
- Collected in person by police or authorised agencies
- Individuals requesting their own data must provide ID
- All disclosures are logged in the CCTV Access Log

12. How the information is used

- To support police investigations
- To support insurance claims
- To respond to Subject Access Requests
- To deter anti-social behaviour

No automated decision-making or profiling**.**

13. Consultation

Consultation was considered. Due to the low risk nature of the system and the absence of high risk processing, formal consultation was not required under ICO DPIA guidance. However, many residents have informally expresses support, and Kent Police encourage its appropriate use and Parish Council Members have approved its use as per Council policies.

14. Lawful basis

- UK GDPR Article 6(1)(e) – Public task
- Processing is necessary for the Council to perform its functions under:
  - Crime and Disorder Act 1998 (s.17)
  - Local Government and Rating Act 1997 (s.31)
  - Criminal Justice and Public Order Act 1994 (s.163)
- Where footage is disclosed to police for crime investigation, processing may also fall under Part 3 DPA 2018 (Law Enforcement Processing).
- No special category data is intentionally processed.

15. Informing the public

- Prominent CCTV signage is displayed
- The Council's CCTV Policy and this DPIA are available on the website
- Signs include contact details for enquiries
- The area is a public space where surveillance is reasonably expected

16. Necessity and proportionality

- Cameras cover only public areas

- No audio, no zoom (as live watching), no analytics
- Access is strictly limited
- Footage is only viewed when necessary
- Retention is limited to 31 days
- Benefits are measured through reduced incidents and police feedback

The system is proportionate to the risks it addresses.

17. Retention period

- 31 days, after which footage is automatically overwritten or memory cards are wiped
- Footage retained for incidents is kept only as long as necessary
- Routine memory card wiping does not require logging

18. Retention procedure

- Automatic overwrite (hard drive)
- Manual wipe (memory card)
- Retention override only when required for:
  - police investigations
  - insurance claims
  - legal proceedings

All overrides are logged

19. Security and integrity

- System stored in a locked cabinet within a locked building
- Password protected access
- Limited authorised personnel
- USBs stored in a safe until collected
- External processors only used under written agreement
- No international transfers

20. Responding to data subject rights

- Requests must be made using the Access Request Form
  - ID required for individuals requesting their own data
  - Council responds within one calendar month
  - Third party identities are blurred
- Requests may be refused if:
  - Insufficient detail is provided
  - Disclosure would prejudice law enforcement
  - Footage has been deleted
  - The request is manifestly unreasonable

21. Less intrusive alternatives considered

- Increased lighting, not feasible due to remote area and cost of installation
- Police patrols not feasible due to resource constraints
- Physical barriers are not appropriate for an open public picnic area and car park.

CCTV is the most effective and proportionate option**.**

22. **Policies, procedures, and auditing**
    - CCTV Policy reviewed annually
    - Access logs maintained for all processing events
    - Internal auditor reviews compliance annually
    - DPIA reviewed annually or when system changes

Risk Assessment Summary

Source of risk and nature of potential impact on individuals	Likelihood of harm	Severity of harm	Overall risk	Measures to control risk
Intrusion into privacy	Possible	Significant	Medium	Cameras only cover public areas; signage; limited access
Incorrect disclosure	Possible	Severe	Medium	Strict authorisation; logging; redaction
Unauthorised access	Remote	Severe	Low	Locked cabinet; password protection
Unauthorised access	Possible	Minimal	Low	Automatic overwrite / routine wipe
Signage removed	Possible	Minimal	Low	Regular checks
Vandalism	Possible	Minimal	Low	Cameras mounted out of reach

It is concluded that the Residual risk: Low

Adopted 07.04.2026

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