Controlled Document

Title	CCTV Policy
Author	Lenham Parish Council
Owner	Lenham Parish Council
Subject	Main Policy Documents
Government Security Classification	Official
Document Version	Version 1
Created	19.08.2025
Approved By	Full Council
Review Date	01.10.2027

Version Control

Version	Date	Author	Description of Change	Sign
1	01.10.2025	Lenham Parish Council	Original Policy	Audrey Ratcliffe

1. Introduction

Lenham Parish Council (LPC) operates a Closed Circuit Television (CCTV) system to ensure a safe and secure environment for residents, staff, councillors, and visitors, as well as to prevent the loss or damage of Council property.

This system is a key component of the Council's efforts to prevent, identify, and reduce crime. LPC owns and manages the CCTV system directly and serves as the system operator and data controller for the images produced.

LPC is registered with the Information Commissioner's Office (ICO) under Registration Number ZB528442.

The CCTV system operates 24 hours a day, 365 days a year, and is monitored as necessary to achieve its stated purposes.

2. Purpose

The purpose of this policy is to regulate the management, operation and use of the CCTV system at LPC. The lawful basis for processing CCTV data under the UK GDPR is LPC's legitimate interests in ensuring public safety, crime prevention, and protection of property. CCTV surveillance at the LPC sites is intended for the purpose of:

a. Protecting LPC buildings and assets, both during and after work hours.
b. Promoting the health and safety of residents, staff, councillors, and visitors by enhancing perceptions of public safety.
c. Prevent bullying and/or intimidation by individuals and/or groups.
d. Reducing the incidence of crime and anti-social behaviour (including theft and vandalism)
e. Supporting Kent Police in the prevention and detection of crime.
f. Assisting in identifying, apprehending and prosecuting offenders.
g. Ensuring that the LPC rules are respected so that the Parish Areas can be properly managed.

The system does not have sound recording capability. Cameras will be maintained to provide clear, usable images for their stated purpose.

The CCTV system is owned and operated by LPC, the deployment of which is determined by LPC members. The introduction of, or changes to CCTV monitoring will be subject to consultation with members of the LPC.

All authorised operators with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are made aware of their responsibilities in following the ICO's CCTV Code of Practice 2021[1]. All members are aware of the restrictions in relation to access to, and disclosure of recorded images.

[1] Surveillance Camera Code of Practice

3. Scope

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. This policy applies to:

a. the Council, its staff and councillors.
b. Contractors and volunteers working on behalf of the Council.
c. Members of the public visiting Council sites.

Non-compliance with this policy may result in disciplinary action, including dismissal. All staff involved in operating the CCTV system will be trained and authorised to ensure proper use consistent with the stated purposes and procedures.

Individuals accessing, recording, or processing CCTV images must possess the necessary skills and training to handle operational, technical, and privacy considerations.

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by LPC. Recognisable images captured by CCTV systems are 'personal data'. They are therefore subject to the provisions of the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

The Parish Clerk is the nominated Responsible Officer for the CCTV system and the main point of contact for all data protection and privacy queries relating to CCTV. In the absence of the Clerk, the Deputy Clerk will assume these responsibilities.

4. Location

The planning and design of the CCTV have endeavored to ensure that the system will give maximum effectiveness and efficiency, but it is not guaranteed that the system will cover or detect every single incident taking place in the areas of coverage. CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by LPC including Equality & Diversity, Code of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including provisions set down in equality and other related legislation.

This policy prohibits monitoring based on the characteristics and classification contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability, etc.

Video monitoring of public areas for security purposes within LPC premises is limited to uses that do not violate the individual's reasonable expectation of privacy. Cameras will not be placed in toilets, changing rooms, private offices, etc. LPC will ensure that all camera positioning is justified, proportionate, and respectful of individuals' privacy.

Please see the map in Appendix B showing the location of CCTV cameras.

5. Covert Monitoring

In liaison with other partners, LPC retains the right in exceptional circumstances to set up covert monitoring. For example:

a. Where there is good cause to suspect that an illegal or serious unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct.
b. Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances, authorisation must be obtained beforehand from the clerk.

Covert Monitoring will cease following completion of an investigation.

6. Storage and retention of CCTV Images

CCTV footage is recorded on secure servers and accessible only to authorised personnel. Recorded data will not be retained for longer than 31 days except where the image identifies an issue and is retained specifically in the context of an investigation/ prosecution of that issue.

Where data is retained for longer than 31 days, an electronic file held on a secure central server where specific CCTV image/recordings are retained will be kept. Neither the UK GDPR nor the Data Protection Act 2018 prescribe fixed retention periods, so footage will be retained only as long as necessary to fulfil its purpose. Therefore, retention will reflect LPC's purposes for recording information and how long it is needed to achieve this purpose. LPC will always store data securely.

7. Access to CCTV Images

Access to live or recorded CCTV footage is restricted to authorised personnel only, as designated by LPC. Supervising the access and maintenance of the CCTV system is the responsibility of LPC.

Every access must be logged before or immediately after accessing footage using the CCTV access log in Appendix D. All fields should be completed in full and use one entry per incident or request. This log must be stored securely and reviewed regularly by the Clerk.

CCTV footage may only be accessed, viewed, or downloaded on devices that are owned and managed by LPC. These devices must meet the Council's security standards and be subject to regular updates and monitoring. The use of personal laptops, phones, tablets, or any non-council-owned equipment to access CCTV footage of public areas is strictly prohibited under any circumstances.

Any data extracted from the CCTV system (e.g. for sharing with law enforcement) must be stored and transmitted securely using council-approved methods and devices.

In the event of a CCTV-related data breach (e.g. unauthorised access, loss, or disclosure of images), the incident must be reported immediately to the Clerk. The Clerk will investigate and record the breach, and, where the breach is likely to result in a risk to the rights and freedoms of individuals, will notify the ICO within 72 hours in line with UK GDPR requirements. Affected individuals will also be notified where there is a high risk to their rights and freedoms.

8. Subject Access Requests (SAR)

a. Individuals have the right to request CCTV footage relating to themselves under the Data Protection Act 2018 and the UK GDPR.
b. All requests should be made by completing the CCTV Access Request Form (available from

the clerk). Individuals submitting requests for access will be asked to provide sufficient information to enable footage relating to them to be identified.

c. LPC does not have a facility to provide copies of CCTV footage but instead the applicant may view the CCTV footage if available.
d. LPC will respond to requests within 28 days of receiving the request.
e. The Council may decline a request if fulfilling it would disclose another person's data, unless consent is provided or disclosure is deemed reasonable under the circumstances.
f. LPC may ask for proof of identity before releasing/viewing footage, to prevent wrongful disclosure.

In addition to the right of access, individuals have the right to:

- request erasure of CCTV data where it is no longer necessary for the purposes collected,
- request restriction of processing, and
- object to processing where LPC is relying on legitimate interests as its lawful basis.

Requests will be considered on a case-by-case basis in line with UK GDPR.

9. Access and Disclosure of images to third parties

There will be no disclosure of recorded data to third parties other than authorised personnel such as the Police and service providers to LPC where there would be a reasonable need to access the data. Disclosure of images to third-parties will only occur when it is required by law or is necessary for crime prevention or detection.

Requests for images must be made to the Clerk using the CCTV Access Request Form, this should include the lawful basis for disclosure. Secure transfer methods must always be used.

If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However, very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then LPC should seek expert advice in the first instance and appropriate legal advice may be required.

The data may be used within LPC's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

The camera locations will be signed up to the Kent Police CCTV Registry.[2] This allows the police to see the location of the cameras, but they cannot access the images without following the procedure above.

Any third-party contractor engaged by LPC to maintain or support the CCTV system will be required to enter into a written data processing agreement compliant with Article 28 of the UK GDPR. This agreement will ensure that contractors:

- process data only on documented instructions from LPC,
- maintain confidentiality and security,
- implement appropriate technical and organisational measures, and
- assist LPC in fulfilling its data protection obligations.

[2] cctvregistrykentandessex.co.uk

10. Fees

In accordance with the UK GDPR, individuals will not normally be charged a fee to exercise their right of access to CCTV data. However, LPC reserves the right to charge a reasonable administrative fee where requests are manifestly unfounded, excessive, or require significant resources for redaction (e.g. removing third-party images). Applicants will be notified of any fee in advance.

11. Responsibilities

LPC retains overall responsibility and will:

a. Ensure that the use of the CCTV systems is implemented in accordance with this policy.
b. Oversee and co-ordinate the use of the CCTV monitoring for safety and security purposes within LPC premises.
c. Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.
d. Ensure that the CCTV monitoring is consistent with the highest standards and protections.
e. Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
f. Maintain a record of access (e.g. an access log) to or the release of any material recorded or stored in the system.
g. Ensure that recordings are not duplicated for release.
h. Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.
i. Give consideration to both LPC members and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
j. Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the LPC and be mindful that no such infringement is likely to take place.
k. Ensure that external cameras are non-intrusive in terms of their position and views of neighbouring residential housing and comply with the principle of “Reasonable Expectation of Privacy”.
l. Where practicable, a second authorised person should be present when using the zoom function to mitigate the risk of misuse.
m. Ensure that camera control is solely to monitor suspicious behavior, criminal damage etc. and not to monitor individual characteristics.
n. Ensure that camera control is not infringing an individuals reasonable expectation of privacy in public areas.
o. Any suspected misuse, technical failure, or security incident involving CCTV must be reported to the Clerk and recorded appropriately.
p. The CCTV system will be regularly tested and maintained, with faults logged and addressed promptly.
q. Regular audits will be carried out at least annually by the Clerk to ensure compliance with this policy.

12. Data protection impact assessments and privacy by design

CCTV has the potential to be intrusive of privacy. LPC will perform a privacy impact assessment when installing or moving CCTV cameras to consider the privacy issues involved with using new surveillance systems to ensure that the use is necessary and proportionate and address a pressing need identified.

A Data Protection Impact Assessment (DPIA) will always be carried out prior to the installation of any new CCTV system or when making significant changes to existing systems. This ensures the use of CCTV is necessary, proportionate, and compliant with data protection legislation.

13. CCTV Signage

It is a requirement of the Data Protection Act to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. LPC is to ensure that this requirement is fulfilled. The CCTV sign should include the following:

a. That the area is covered by CCTV surveillance and pictures are recorded.
b. The purposes of using CCTV.
c. The name of the Parish Council.
d. The contact telephone number or address for enquiries.

An example sign can be seen in Appendix A.

14. Policy Review

The Clerk is responsible for monitoring and reviewing this policy. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

15. Links with other policies

This CCTV policy links with LPC's:

- Data Protection Policy
- Freedom of Information Policy CCTV
- CCTV Access Request Policy
- Information Security Policy
- Complaints Policy and Procedure

Appendix A - Example Sign

Notices & Images are being recorded for the purpose of preventing crime and ensuring public safety.

This system will be in operation 24 hours a day, every day. These images may be passed to the police.

This scheme is controlled by Lenham Parish Council

Data is held securely and accessed only by authorised personnel. For more information contact Lenham Parish Council on 01622 829034

Appendix B – Map of CCTV locations

To be agreed:

Appendix C: Definitions/glossary of terms

CCTV (Closed Circuit Television):
A surveillance system using video cameras to transmit a signal to a specific place, typically for monitoring and security.

CCTV Operator – any authorised LPC staff or councillor trained and permitted to operate the CCTV system.

Data Controller:
The organisation or individual who determines the purpose and means of processing personal data. LPC is the Data Controller for its CCTV system.

Data Processor:
An external individual or organisation that processes personal data on behalf of the Data Controller (e.g. the CCTV maintenance provider).

Data Subject:
An identifiable individual whose personal data is being collected, held, or processed (e.g. anyone recorded by the CCTV system).

UK GDPR (UK General Data Protection Regulation):
The UK's primary data protection legislation, governing how personal data is collected, processed, and stored.

Data Protection Act 2018 (DPA 2018):
UK law that supplements the UK GDPR and outlines additional national rules on data processing and protection.

Personal Data:
Any information that can identify a living individual, either directly or indirectly. In CCTV, this includes identifiable images or video footage.

Subject Access Request (SAR):
A formal request from an individual to access their personal data held by an organisation, including CCTV footage that features them.

Reasonable Expectation of Privacy:
The expectation that individuals have to not be observed in certain situations (e.g. inside private residences or restrooms). CCTV must not infringe on these areas.

Covert Surveillance:
Monitoring without the knowledge of individuals, permitted only in exceptional circumstances such as the prevention or detection of serious crime, and subject to strict authorisation.

Retention Period:
The amount of time CCTV footage is stored before being securely deleted. For Lenham Parish Council, this is typically 31 days unless required for investigation.

Access Log:
A record that documents when, why, and by whom CCTV footage has been accessed or shared. Used for auditing and accountability.

Data Breach:
Any unauthorised access, loss, alteration, or disclosure of personal data, including CCTV footage.

Surveillance Camera Code of Practice:
Statutory guidance under the Protection of Freedoms Act 2012, issued by the Surveillance Camera Commissioner, setting out best practices for using CCTV in public spaces.

Appendix D – CCTV Access log

The access log will be kept on the LPC one drive in the CCTV folder.

Log No.	Date of Access	Time of Access	Name of Person Accessing Footage	Position/Role	Reason for Access	Location/Camera Accessed	Footage Date/Time Range	Access Type (View/ Download/ Copy)	Authorised By	Notes/ Actions Taken	Signature

Procedure for CCTV/ wif-fi issues.

ISSUE	PROCEDURE	OTHER INFO.
Camera/s off line	1. Check the camera in back office 2. Call Orbital 3. Camera issue, call Amiga	
Camera broken	1. Call Amiga	

- Orbital can dial in and see if it's a camera or connection issue.

IMPORTANT NUMBERS:
Orbital 01227 668900 (option 2)
Amiga 01622 725225
George (Pavillion access) 07969 834491