CCTV Code of Practice

Adopted by Ruskington Parish Council on 13 May 2025
Minute Ref: 12.6., page 40 -2025-AMPC
To be reviewed in April 2026

Overview: A Code of Practice for the Council's management and use of CCTV and the release of images, in compliance with UK law.

CCTV footage of identifiable people is considered personal data and is governed by:

• The UK GDPR and the Data Protection Act 2018

• The Protection of Freedoms Act 2012

• Human Rights Act 1998 (Article 8)

CCTV images must not be released (except to the Police in lawful circumstances) or shared publicly by Council without the individual's consent. Images can only be shared by the Police in certain circumstances and following their own law enforcement procedures.

Public sharing, and publicly identifying children, even indirectly, is unlawful. (LALC, 7 April 2025).

Management of the System

Normal operational responsibility of the scheme will be by nominated Councillors as per the Councillors' published roles. In the absence of these nominated Councillors, responsibility will revert to the Chairman and the Clerk, and in the Clerk's absence, the Chairman and Deputy Clerk.

Global Vision (CCTV) Limited, Unit 0, Peregrine Mews, Dowding Road, Allenby Trading Estate, Lincoln. LN3 4PH, who carried out the installation, can access the system for any annual maintenance or essential repairs with the permission of the Clerk, Deputy Clerk, or nominated Councillors.

The Pavilion CCTV system is located in a locked cabinet in the Pavilion, and the Parish Office CCTV system is located in a secure room at Ruskington Parish Office. Access to the CCTV images is limited to the following Council positions:

- Any Councillor, formally accompanied by the Clerk or Deputy Clerk, with a legitimate and known reason for viewing the footage, in lawful pursuit of Council business.
- Clerk to Ruskington Parish Council.
- Deputy Clerk & RFO to Ruskington Parish Council.

On the advice of LALC, the CCTV footage can be used to support disciplinary investigations.

Breaches of this policy will be investigated by the Clerk and reported to the Parish Council.

A CCTV system prevents crime largely by increasing the risk of detection and prosecution of an offender. Any relevant digital evidence must be in acceptable format for use at court hearings. This policy must be read and understood by all persons involved in this scheme and individual copies of the policy will therefore be issued for retention. A copy of the policy will also be available for reference in the CCTV system cabinets and on the Parish Council's website.

Control and Operation of the Camera, Monitor and System

Operators must strictly observe the following points:

1. Authorised operators must act with due probity and not abuse the equipment or change the pre-set criteria to compromise the privacy of an individual.
2. The position of the camera and monitor have been agreed following consultation with the Police and security consultants in order to comply with the needs of the public.
3. No public access will be allowed to the monitor.
4. Releasing and sharing of CCTV footage on Council's communication channels or to the media is not permitted.
5. The Police are permitted access to recording media and images if they have reason to believe that such access is necessary to investigate, detect or prevent crime. The Police are able to visit the secure recording area to review and confirm the Parish Council's operation of CCTV arrangements. Any visit by the Police to view images will be arranged through and logged by the Clerk or Deputy Clerk. If the Police decide to release any footage, they do so in accordance with their own legal procedures and Council is not permitted to share this.
6. Operators should check the accuracy of the date/time display on the CCTV system on a monthly basis.
7. Digital records should be securely stored to comply with data protection and should be handled by the essentially minimum number of persons. Digital images will be automatically erased from the system after a period of 28 days. Any images that are downloaded from the system to a secure storage device, in the case of vandalism or crime, for example, will be erased after a maximum period of 6-months or, completion of the investigation, whichever is the latter.
8. Should any digital records be required as evidence at Court, persons handling such record may be required to make a statement to a Police officer and sign an exhibit label. Any extracted data that is handed to a Police officer should be signed for by the officer and information logged to identify the recording and showing the officer's name and Police station. The log should also show when such information is returned to the Parish Council by the Police and/or the outcome of its use.
9. Any event that requires checking of recorded data should be clearly detailed in the log book of incidents, including crime numbers, if appropriate and the Parish Council notified at the next available opportunity.
10. Any damage to equipment or malfunction discovered by the Clerk or Deputy should be reported to the Parish Council, the appropriate repairs actioned, and the call logged showing the outcome. When a repair has been made this should also be logged showing the date and time of completion.
11. Any request by an individual member of the public for access to their own recorded image must be made on the 'Access Request Form' detailed at Annex A, and is subject to a standard fee in-line with the Council's Communication / Publication Policy. Forms are available from the Clerk and will be submitted to the Parish Council for consideration and reply, normally within 40 calendar days of receiving the request.

Accountability

The Council's Policy and Code of Practice are based on UK law and the guiding principles of the Surveillance Camera Code of Practice (.gov.uk website). A copy of the guiding principles is detailed at Annex B.

Copies of the CCTV Policy are available in accordance with current GDPR, Freedom of Information Act, and the Council's Data Publication Policy, as will any reports that are submitted to the Parish Council providing it does not breach security needs, and will be responded to within 20 working days from receipt of the request.

The Police will be informed of the installation and provided with a copy of this CCTV Policy. Any written concerns or complaints regarding the use of the system will be considered by the Parish Council, in line with the existing complaints policy.

ANNEX A

Ruskington Parish Council
CCTV Images Access Request Form

Date of Recording	Time of Recording	Place of Recording

Applicants name and address Postcode Telephone Email	Description of applicant and any distinguishing features (e.g. clothing) plus a recent photograph to aid identification, if necessary.
Signature of applicant	(or parent/guardian if under 18)

Received by	Clerk/Councillor signature	Date and time received

Fee charged	Fee paid	Request approved by Parish Council Yes / No	Date applicant informed

ANNEX B

SURVEILLANCE CAMERA CODE OF PRACTICE

Available in full at:

https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version [Date accessed 15/4/2025]

System operators should adopt the following 12 guiding principles:

Guiding Principles

System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.