

CCTV Code of Practice



V1. Revised and updated in July 2026 to reflect current CCTV and data protection requirements.

Adopted by Ruskington Parish Council on 14 July 2026

Minute Ref: 8.2., page 408-2026

To be reviewed in April 2029, or sooner if legislation, guidance, system use or risk changes.

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 personal data. The Council will operate CCTV lawfully, fairly and transparently, and only where its use is necessary and proportionate for the stated purposes. The Council will comply with the following legal and regulatory framework, as amended from time to time:

- The UK GDPR and the Data Protection Act 2018
- The Data (Use and Access) Act 2025, insofar as it amends or supplements UK data protection law
- The Protection of Freedoms Act 2012
- Human Rights Act 1998 (Article 8)
- The Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012, where applicable to relevant authorities in England and Wales

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

Particular care must be taken where CCTV images include children or vulnerable people. Such images must not be shared publicly, or used to identify individuals, directly or indirectly, unless there is a clear lawful basis and appropriate safeguarding, data protection and proportionality considerations have been documented.

The Council is the data controller for CCTV operated by or on behalf of the Council. The lawful basis for processing CCTV images will normally be public task, where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority. Where another lawful basis is relied on for a specific use, this must be documented before processing takes place.

Before installing new cameras or materially changing the use, location, coverage or purpose of any CCTV system, the Council will complete and record a Data Protection Impact Assessment or equivalent privacy assessment. The assessment will consider necessity, proportionality, privacy impact, risks to individuals, retention, access controls, signage and whether less intrusive alternatives are available.

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, may access the system for annual maintenance or essential repairs only with the permission of the Clerk, Deputy Clerk, or nominated Councillors. Any contractor access must be limited to what is necessary, authorised in advance, logged, and subject to appropriate confidentiality, security and data protection obligations.

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:

Clear and visible signs will be displayed where CCTV is in operation. Signs should be readable, placed where people are likely to see them before or as they enter the area being monitored, and should state that CCTV is in use, the purpose of the recording and a contact point for enquiries, subject access requests and complaints.

- Councillors may view footage only where this is necessary for a specific Council function, investigation, complaint, insurance or legal matter, disciplinary matter, or other lawful Council purpose. Viewing must be formally arranged with and accompanied by the Clerk or Deputy Clerk, and each viewing must be recorded in the CCTV log.
- Clerk to Ruskington Parish Council.
- Deputy Clerk & RFO to Ruskington Parish Council.

CCTV footage may be used to support disciplinary investigations only where its use is necessary, proportionate, relevant to the matter under investigation, and consistent with the Council's employment, disciplinary and data protection policies.

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. Cameras must be positioned and reviewed so that they monitor only the areas necessary for the stated purpose. Cameras must not be directed at areas where individuals would have a higher expectation of privacy unless this is strictly necessary, lawful, proportionate and documented.
4. No public access will be allowed to the monitor.

5. Releasing and sharing of CCTV footage on Council's communication channels or to the media is not permitted.
6. 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.
7. Operators should check the accuracy of the date/time display on the CCTV system on a monthly basis.
8. Digital records should be securely stored to comply with data protection law and should be handled by the minimum number of authorised persons necessary. Digital images will normally be automatically erased from the system after 28 days, unless retention for a longer period is necessary for a specific, documented purpose such as the investigation of an incident, crime, complaint, insurance matter, disciplinary matter or legal claim. Any images downloaded from the system to a secure storage device will be retained only for as long as necessary for the documented purpose and will be erased when that purpose has been discharged, unless a longer retention period is legally required.
9. 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.
10. All viewing, downloading, copying or disclosure of CCTV footage must be recorded in a disclosure or access log. The log should include the date and time, person authorising access, person viewing or receiving the footage, reason and lawful basis, camera/location, period of footage, method of transfer, any crime or incident reference, and the deletion, return or outcome date where applicable.
11. 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.
12. 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.
13. Any request by an individual for access to CCTV images of themselves will be treated as a subject access request under data protection law. A request may be made in writing or verbally and should provide enough information to help the Council identify the relevant footage, such as the date, time, location, description of the individual and proof of identity where reasonably required. The Council will normally respond free of charge and within one calendar month of receiving the request, unless data protection law permits an extension or a charge because the request is manifestly unfounded, excessive or repetitive. Footage may be withheld, redacted, restricted to a viewing, or refused where disclosure would identify other individuals, prejudice an investigation, or where another lawful exemption applies.

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](http://www.gov.uk) website). A copy of the guiding principles is detailed at Annex B.

The Council will keep a record of CCTV processing activities, including the purpose of the system, camera locations, areas covered, access permissions, retention arrangements, disclosures, incidents, requests and reviews. CCTV arrangements will be reviewed at least annually, and sooner if there is a material change in the system, purpose, law, guidance or risk.

Copies of the CCTV Policy, non-personal information about the system, and reports submitted to the Parish Council will be made available in accordance with the Freedom of Information Act 2000, the Council's Publication Scheme and the Council's Data Publication Policy, provided disclosure does not breach security, confidentiality or data protection requirements. Freedom of Information requests will normally be responded to within 20 working days. Requests by individuals for CCTV images of themselves will be handled separately as subject access requests under UK data protection law and will normally be responded to within one calendar month. Images of other individuals within the footage must be erased or blurred unless they have provided written permission for their image to be shared.

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 Council's complaints policy and data protection complaints procedure. Individuals should be told how to contact the Council about CCTV concerns and that they may complain to the Information Commissioner's Office if they remain dissatisfied with how their personal data has been handled.

ANNEX A

Ruskington Parish Council CCTV Images Access Request Form

Date of Recording		Time of Recording		Place of Recording	
Applicants name and address			Description of applicant and any distinguishing features (e.g. clothing) plus a recent photograph to aid identification, if necessary.		
Postcode					
Telephone					
Email					
Signature of applicant			(or parent/guardian if under 18)		
Received by		Clerk/Councillor signature		Date and time received Deadline for response: one calendar month from receipt, unless extended in accordance with data protection law.	
Fee charged, if applicable under data protection law	Reason for fee, if charged	Request reviewed by Clerk / authorised officer Disclosed / Refused / Restricted		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 01/06/2026]

System operators should adopt the following 12 guiding principles:

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.