

UPTON & NORTH ELMSALL PARISH COUNCIL

CCTV POLICY

Introduction

Upton and North Elmsall Parish Council uses closed-circuit television (CCTV) at the Village Hall, Harewood Lane, Upton, Pontefract, WF9 1JB, for the purposes of site security, public safety, crime prevention and the protection of Council property.

The Council currently operates approximately 20 CCTV cameras around the Village Hall site. The system is used for security purposes only. The cameras do not record audio and are not used for general monitoring of staff, councillors, hirers, allotment holders, visitors or members of the public.

The CCTV system is locally based. Access to the physical system is restricted to the Parish Clerk. The system does not have remote access functionality.

As part of the 2026 policy review, audio recording on the Village Hall CCTV system was disabled so that the system records images only.

Security cameras are also installed at other Council-owned sites, including the Community Garden, School Street, Harewood Lane allotments and stables blocks. Where such cameras remain in place, they are also covered by this policy. Where access arrangements, account ownership or system controls are unclear, the Clerk will review the equipment and report to Council as appropriate, with a view to removing, replacing or regularising those systems.

This policy explains how the Council manages CCTV and recorded images in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018, the Council's wider data protection policies and relevant guidance issued by the Information Commissioner's Office.

Purpose Of CCTV

The Council uses CCTV for the following purposes:

- to help protect Council buildings, land, assets and equipment;
- to help deter, prevent and detect crime, vandalism, anti-social behaviour and unauthorised access;
- to support the safety and security of staff, councillors, volunteers, hirers, contractors, visitors and members of the public using Council facilities;
- to assist the Police or other lawful authorities where footage is relevant to the prevention or detection of crime, public safety, legal proceedings or another lawful purpose;
- to support the Council in investigating incidents involving Council property, premises or facilities.

CCTV will not be used for any purpose that is incompatible with the above. It will not be used for covert monitoring, routine staff supervision, or to intrude unnecessarily into the private lives of individuals.

Lawful Basis For Processing

Images captured by CCTV may identify individuals and are therefore personal data.

Adopted On: 19th May 2026

The Council's lawful basis for processing CCTV images is Article 6(1)(e) of the UK GDPR: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council.

The Council may also rely on Article 6(1)(f), legitimate interests, where appropriate in relation to the protection of Council property and assets, although this will not apply where the Council is carrying out its public tasks as a public authority.

The Council does not use CCTV for facial recognition, biometric identification, audio recording or automated decision-making.

Data Protection Principles

The Council will ensure that CCTV images are:

- processed lawfully, fairly and transparently;
- collected only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- kept accurate where relevant, including through reasonable checks on system date and time settings;
- kept for no longer than necessary;
- stored securely and protected against unauthorised access, loss, misuse or disclosure.

Responsibility For The System

The Parish Council remains the data controller for CCTV operated on its behalf.

Day-to-day responsibility for the management of CCTV rests with the Parish Clerk.

The Clerk is responsible for:

- ensuring that access to the system is appropriately restricted;
- ensuring that CCTV signage is in place where required;
- checking, where practicable, that the system is operating correctly;
- arranging maintenance, replacement or removal of CCTV equipment where required;
- keeping appropriate records of access, disclosure, incidents and requests;
- ensuring that requests for footage are handled in line with data protection legislation and this policy.

Any significant changes to the CCTV system, including new cameras, new locations, remote access arrangements, audio recording, or a change in the purpose of CCTV use, must be considered by Full Council before implementation, unless urgent action is required to protect Council property or public safety. Any urgent action must be reported to the next available Council meeting.

Camera Locations And Privacy

Cameras will be positioned to cover only areas that are necessary for the stated purposes of this policy.

The Council will avoid, as far as reasonably practicable, capturing areas where individuals would have a higher expectation of privacy.

Cameras must not be positioned to deliberately record private homes, gardens, internal areas not connected to the security purpose, or neighbouring land beyond what is unavoidable for site security. CCTV must not be installed in toilets, changing areas or any other area where individuals would reasonably expect privacy.

Where any new camera is proposed, the Council will consider whether CCTV is necessary and proportionate, whether less intrusive measures would be sufficient, and whether the camera position should be adjusted to minimise privacy impact.

Signage And Transparency

Clear CCTV signage will be displayed at appropriate points where CCTV is in operation. Signs should, as far as reasonably practicable, make clear:

- that CCTV is in use;
- that Upton and North Elmsall Parish Council is responsible for the system;
- the purpose of the CCTV;
- how to contact the Council about the system.

A copy of this policy will be made available on request and published on the Council's website.

Access To CCTV Footage

Access to CCTV footage is restricted to the Parish Clerk, unless access is required for a lawful and appropriate reason.

Footage may be viewed or extracted only where there is a legitimate reason to do so, such as:

- investigating damage, theft, vandalism, unauthorised access, anti-social behaviour, an accident, a safeguarding concern or another incident;
- responding to a request from the Police or another lawful authority;
- responding to a subject access request;
- obtaining evidence for legal, insurance or regulatory purposes;
- checking system operation, maintenance or security.

Where the Parish Clerk accesses CCTV footage, the Chair of the Council must be notified that access has taken place. This notification will be for audit and oversight purposes only and will record the date and time of access. The Chair does not need to be provided with details of the footage viewed, the individuals involved, or the reason for access unless there is a lawful and appropriate reason for this information to be shared.

The Parish Clerk must maintain a confidential paper record of all access to CCTV footage. The record should include:

- the date and time the footage was accessed;
- the name of the person accessing the footage;
- the reason for access;
- the date and time period of footage viewed or extracted;
- whether any footage was copied, downloaded, disclosed or provided to a third party;
- who the footage was disclosed to, where applicable;
- confirmation that the Chair of the Council was notified of the access.

The CCTV access record must be kept securely and made available to the Council, the Data Protection Officer, internal auditor, external auditor, Police, Information Commissioner's Office or other lawful authority where required.

Footage must not be viewed out of curiosity or for personal reasons. Unauthorised viewing, copying, disclosure or use of CCTV footage will be treated as a serious matter and may be reported to the Council.

Retention Of Footage

CCTV footage will normally be retained for up to 28 days, unless the system automatically overwrites footage sooner or a longer retention period is necessary for a specific lawful reason.

Footage may be retained for longer where it is required for:

- an ongoing investigation;
- a request from the Police or another lawful authority;
- legal, insurance or disciplinary proceedings;
- a subject access request;
- another lawful and documented purpose.

Where footage is retained beyond the normal retention period, the reason must be recorded. Once it is no longer required, it must be securely deleted or allowed to be overwritten.

The Council will not keep footage simply because it may be useful in the future.

Disclosure Of Footage

CCTV footage will not be disclosed to third parties unless there is a lawful reason to do so.

Footage may be disclosed to:

- the Police or other law enforcement agencies;
- the Council's insurers or legal advisers;
- a court, tribunal or regulatory body;
- another organisation or individual where disclosure is required by law or is necessary and proportionate for a legitimate purpose.

Any disclosure must be authorised by the Clerk and recorded, including:

- the date of disclosure;
- the name and organisation of the person receiving the footage;
- the reason for disclosure;
- details of the footage disclosed;
- how the footage was provided;
- any crime reference number or case reference, where applicable.

Footage will not normally be released to the media or posted online. Any such disclosure would only be considered in exceptional circumstances, normally on the advice of the Police or legal advisers, and where it is lawful, necessary and proportionate.

Subject Access Requests

Individuals have the right to request access to personal data held about them, including CCTV footage in which they are identifiable.

Requests should be made in writing to the Parish Clerk. The Council may ask the requester to provide:

- the date, time and location of the recording;
- a description of the incident or footage requested;
- information to help identify the requester in the footage;
- proof of identity, where required.

The Council will respond to subject access requests without undue delay and normally within one month, in accordance with data protection legislation.

Before providing footage, the Council will consider whether it contains images of other identifiable individuals. Where necessary, footage may be redacted, still images may be provided instead, or the request may be refused or limited where disclosure would adversely affect the rights and freedoms of others or prejudice an investigation.

No fee will normally be charged for a subject access request, unless the request is manifestly unfounded, excessive or repetitive, in which case the Council may act in accordance with data protection legislation.

Security Of The System And Footage

The Council will take reasonable steps to protect CCTV footage against unauthorised access, loss, misuse, alteration or disclosure.

This may include:

- restricting physical access to recording equipment;
- using passwords or other access controls where available;
- ensuring access is limited to those who need it;
- keeping downloaded footage securely;
- using secure transfer methods where footage is disclosed;
- ensuring any contractor or service provider involved in the system provides appropriate security assurances;
- reviewing access arrangements where equipment is replaced or upgraded.

Where any CCTV system is found to have unclear account ownership, unknown passwords, unnecessary remote access or insufficient security controls, the Clerk will take reasonable steps to secure, disable, remove or replace the system as appropriate.

Maintenance And Faults

The Clerk will arrange for CCTV equipment to be maintained, repaired, replaced or removed where necessary and within the Council's usual financial and procurement arrangements.

Any fault, damage or malfunction identified with CCTV equipment should be recorded and addressed as soon as reasonably practicable, taking into account the level of risk to the site concerned.

Data Breaches

Any suspected data breach involving CCTV, including unauthorised access, loss, disclosure or misuse of footage, must be reported to the Clerk as soon as possible.

The Clerk will assess the incident in accordance with the Council's data protection procedures and determine whether the breach needs to be reported to the Information Commissioner's Office and/or affected individuals.

Complaints

Any concerns or complaints about the Council's use of CCTV should be made to the Parish Clerk in the first instance.

Complaints will be considered in accordance with the Council's Complaints Policy, where applicable. Individuals also have the right to raise concerns with the Information Commissioner's Office.

Operational Records

The Council will maintain appropriate internal records to support the operation of the CCTV system, including records of access to footage, disclosure of footage, subject access requests, system faults, maintenance and periodic reviews.

These records will be retained securely and will not be published, as they may contain personal data, security-sensitive information or details relating to incidents or investigations.

Review

This policy will be reviewed periodically, usually at least once during each municipal year, or sooner if:

- there is a significant change to the CCTV system;
- cameras are added, removed or replaced;
- the purpose of CCTV use changes;
- there is a change in relevant legislation or guidance;
- an incident, complaint or data protection concern indicates that a review is required.

As part of the review, the Council will consider whether the CCTV remains necessary and proportionate, whether camera coverage remains appropriate, whether signage is adequate, and whether access and retention arrangements remain suitable.