

MARKYATE PARISH COUNCIL



Parish Office, Y2K Hall, Cavendish Road, Markyate, Herts. AL3 8PS
01582 840110
clerk@markyateparishcouncil.gov.uk www.markyateparishcouncil.gov.uk
Clerk to the Council: Mrs V Tilley

CCTV Policy

Policy Updated: March 2026

Next Review Date: March 2027

1. Introduction and Statement of Intent

1.1. Markyate Parish Council (MPC) uses Closed-Circuit Television (CCTV) to ensure the safety and security of staff, visitors and property.

1.2. This policy regulates the management, operation, and use of the system in compliance with the UK GDPR and Data Protection Act 2018.

1.3. CCTV will be operated with respect for privacy, ensuring a balance between security objectives and individual rights.

1.4. The system will not be used to monitor employees in private areas (e.g., toilets, break rooms) or for non-legitimate purposes.

2. Purposes of CCTV

The CCTV system is installed for the following purposes:

- To promote a safe environment for staff, users, and visitors.
- To protect the building and assets from crime, vandalism, and damage.
- To deter and detect criminality and support law enforcement.
- To assist in the investigation of accidents or health and safety incidents.
- To assist in disciplinary or grievance procedures.

3. Data Protection and Compliance

3.1. **Lawful Basis:** The processing of CCTV data is necessary for the performance of a task carried out in the public interest or for the legitimate interests of the organisation.

3.2. **Transparency:** Signs are displayed in and around the building notifying individuals they being monitored.

3.3. **Registration:** The council is registered with the Information Commissioner's Office (ICO) where required.

4. Operational Procedures

4.1. **System Control:** The CCTV installed at Markyate Village/Y2k Hall and the images produced by it are controlled by the Parish Council who are responsible for how the system is used. Day to day operational responsibility lies with The Clerk who reports directly to Markyate Parish Council.

4.2. **Monitoring:** Cameras are not used for continuous, real-time monitoring of staff performance.

MARKYATE PARISH COUNCIL

5. Retention and Security of Data

5.1. **Retention Period:** Recorded images will be retained for a maximum of 28 days before being automatically overwritten, unless required for an ongoing investigation.

5.2. **Security:** Recorded footage is stored in a secure, restricted area with limited access.

5.3. **Encryption:** All footage is password-protected and encrypted where possible.

6. Access to CCTV Images

6.1. **Access Requests:** Access to, or disclosure of, images is strictly limited to authorized personnel.

6.2. **Internal Access:** Authorized staff may view footage for investigation purposes, documented in an Access Log.

6.3. **External Disclosure:** Images will only be released to law enforcement (e.g., Police, fly tipping investigations) or in response to legal proceedings.

6.4. **Subject Access Requests (SAR):** Individuals have the right to request access to CCTV footage of themselves under the General Data Protection Regulation.

All requests for access should be made in writing or email to The Clerk providing sufficient information to enable the footage relating to them to be identified i.e. date, time, and location. Such requests will be handled within one month of receiving the written request.

All requests for access are recorded. If disclosure is denied, the reason is documented and the individual will be informed within no more than 30 days of the reason and their right to complain to a statutory authority. MPC reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

A fee of £15 may be charged for a Subject Access Request, depending on circumstances.

7. Complaints

Enquiries or Complaints about the operation of the CCTV system should be directed to The Clerk clerk@markyateparishcouncil.gov.uk in accordance with the organisation's complaint procedure.

8. Monitoring and Review

This policy will be reviewed annually or when significant changes are implemented to ensure it remains compliant with legislation and best practices.

Checklist for Implementation (2026)

- **[] DPIA Conducted:** Ensure a Data Protection Impact Assessment is filed.
- **[] Signage:** Verify clear, visible signs are placed at all entry points.
- **[] Staff Training:** Ensure staff managing the system are trained on privacy and security.
- **[] Log Access:** Maintain an Access Log for all downloads/viewings.
- **[] Retention Check:** Confirm the automatic deletion/overwriting is functioning.