

CCTV Policy

Original Policy by **Bindesh Majithia**

Updated
May 2026



Contents

Introduction and Background	2
Purpose.....	2
Scope.....	2
Legal Framework.....	2
Associated Policies	3
Statement of Principle	3
Roles and Responsibilities	3
Purpose and Use of CCTV	3
Use of CCTV by Kashrut	3
Live Monitoring and Recording	4
Transparency and Signage	4
Retention and Storage	4
Access, Disclosure and Sharing	4
Law Enforcement Requests	4
Data Subject Access Requests (DSARs)	4
Third Party Disclosures	4
Data Security	4
Complaints.....	5
Monitoring and Review.....	5

US CCTV Policy

Introduction and Background

The United Synagogue operates Closed Circuit Television (CCTV) systems across a number of its offices, Synagogues, and other premises, to support the safety and security of its members, staff, visitors, residents, property, and the wider community. CCTV plays a vital role in deterring and detecting crime, responding to security incidents, and safeguarding those who use or work within United Synagogue premises.

CCTV systems operate across a diverse estate, including head office, synagogues, cemeteries, and certain residential and licensee properties. In respect of non-residential premises, CCTV monitoring arrangements are delivered in partnership with the Community Security Trust (CST), reflecting their shared responsibility for security within the wider Jewish community.

Purpose

This policy is intended to provide a clear and consistent framework for the lawful and proportionate use of CCTV, ensuring that security and operational needs are balanced appropriately with individuals' rights to privacy and data protection. It sets out the lawful basis for the use of CCTV across United Synagogue premises, governance and operation of CCTV systems, joint controller arrangements with Kashrut licensees and CST, access and disclosure requirements, and the rights of individuals whose personal data is captured.

Scope

This policy applies to CCTV systems operating at United Synagogue Head Office, all member synagogues, cemeteries, Kashrut licensee premises, and United Synagogue owned or managed residential and other properties. It applies to staff, volunteers, members, residents, contractors, and visitors.

Legal Framework

This policy is informed by and operates within the framework of UK employment and privacy legislation and relevant guidance, including but not limited to the following:

- [UK General Data Protection Regulation](#) (UK GDPR)
- [Data Protection Act 2018](#)
- [Human Rights Act 1998](#)
- [Protection of Freedoms Act 2012](#) (Surveillance Camera Code of Practice)
- [ICO Guidance on Video Surveillance \(CCTV and similar technologies\)](#).

CCTV footage constitutes personal data where individuals are identifiable, and is processed in accordance with data protection principles. The lawful basis relied upon is legitimate interests, Article 6(1)(f)) UK GDPR. Appropriate Data Protection Impact Assessments (DPIAs) are completed, retained, and reviewed where required under Article 35 UK GDPR. References to CCTV in this policy include the related audio recordings.

Associated Policies

This policy is intended to complement, and should be read alongside, the Charity's wider Data Protection and Privacy related policies, including.

- [Data Protection Policy](#)
- [Confidentiality Policy](#)
- [Safeguarding Policies](#)
- [Data Retention Policy](#)
- [Privacy Policy](#)

Statement of Principle

The United Synagogue recognises that the use of CCTV involves the processing of personal data and, as such, must be managed with care, transparency, and accountability.

The Charity is committed to ensuring the safety and security of its members, employees, volunteers, visitors, and property, while respecting the rights and freedoms of individuals, including their right to privacy.

CCTV systems are used in a proportionate, lawful, and transparent manner, and only where necessary for legitimate purposes. All CCTV activity is carried out in accordance with UK data protection legislation, the Information Commissioner's Office (ICO) Guidance on Video Surveillance, and relevant best practice guidance.

Roles and Responsibilities

The United Synagogue is a data controller for all CCTV systems operated across its premises. For Kashrut licensee premises, the Charity is joint data controller, with each respective licensee, this provision is a condition of all standard Kashrut licensee agreements. For all non-residential United Synagogue premises, the Charity and CST act as joint data controllers.

A written joint controller arrangement is in place, setting out respective responsibilities, including lawful basis determination, transparency, data security, handling of data subject rights, and cooperation with regulators.

Purpose and Use of CCTV

CCTV is primarily used for crime prevention and detection, safeguarding, protection of individuals, and protection of United Synagogue property and assets. CCTV must not be used for routine monitoring of employee performance, nor installed in areas where individuals have a reasonable expectation of privacy.

Use of CCTV by Kashrut

CCTV is installed in the food preparation areas at licensee premises and periodically monitored by the Kashrut supervisory team. Monitoring is limited, proportionate, and conducted only where necessary to verify compliance with kosher food preparation standards. Footage is not used for routine staff performance management, disciplinary purposes, or continuous monitoring of individuals. Each respective licensee is a joint data controller with the United Synagogue, in respect of CCTV footage taken at or from their respective premises.

Live Monitoring and Recording

CCTV systems may operate continuously and may be subject to live monitoring and recording. For non residential premises, live remote monitoring is carried out centrally by CST.

Access to live feeds and recorded footage is restricted to authorised personnel only, subject to role-based access controls and audit logging. Access logs are regularly reviewed, and misuse of CCTV systems may result in disciplinary or contractual action.

Transparency and Signage

Appropriate and clearly visible signage must be displayed at all CCTV monitored premises, informing individuals that CCTV is in operation, the purpose of processing, the identity of the data controller, and how further information can be obtained.

Retention and Storage

CCTV footage is retained only for as long as necessary, to achieve the stated purposes. Standard retention periods are set out in the [Data Retention Policy](#) and reviewed regularly. Footage relating to incidents, investigations or legal proceedings, may be retained for longer where lawful and justified. All footage is stored securely using appropriate technical and organisational measures.

Access, Disclosure and Sharing

Access to CCTV footage is restricted to authorised personnel, and must be necessary, lawful, and proportionate. All access and disclosures must be recorded.

Law Enforcement Requests

Footage may be disclosed to the police or other competent authorities, where a lawful request is made, and disclosure is necessary for the prevention or detection of crime, or the apprehension or prosecution of offenders. Requests must be documented and assessed and approved by the Data Protection Officer or a nominated senior officer.

Data Subject Access Requests (DSARs)

Individuals have the right to request access to CCTV footage containing their personal data. Requests may be made in writing and will be processed in accordance with statutory timescales. Identity will be verified and footage reviewed and redacted as necessary, to protect the rights of third parties. CST will provide reasonable assistance for footage falling under joint control.

Third Party Disclosures

Footage will not be disclosed to third parties, unless disclosure is required by law, necessary to prevent or detect crime, required in connection with legal proceedings, or otherwise permitted under data protection legislation.

Data Security

The Charity implements appropriate technical and organisational measures to protect CCTV data, including secure systems, encryption where appropriate, restricted access controls, and data breach reporting and management procedures.

Complaints

Individuals who have concerns regarding the use of CCTV, may raise them with the Data Protection Officer dpo@theus.org.uk. Where concerns cannot be resolved internally, individuals have the right to lodge a complaint with the Information Commissioner's Office.

Monitoring and Review

This policy will be reviewed at least every two years, or more frequently where required, due to changes in legislation, regulatory guidance, or operational practice.