HASLEMERE TOWN COUNCIL

CCTV POLICY

Contents

1. Purpose

Haslemere Town Council operates closed-circuit television systems ("CCTV") for specified, lawful and proportionate purposes connected with the prevention and detection of crime, public safety, staff and visitor safety, and the protection of Council premises, land, facilities and assets.

This policy explains how the Council manages CCTV in accordance with data protection legislation, information governance requirements and good practice.

2. Scope

This policy applies to all CCTV systems operated by, or on behalf of, Haslemere Town Council. It applies to:

- fixed CCTV cameras;
- recorded images;
- live monitoring, where applicable;
- downloaded or exported footage;
- CCTV footage disclosed to third parties;
- staff, councillors, contractors and volunteers who may have access to CCTV systems or footage.

This policy does not authorise covert surveillance, audio recording, facial recognition, ANPR, biometric analytics or behavioural analytics. These will not be used unless separately approved by the Council following a Data Protection Impact Assessment and DPO review.

3. Legal framework

The Council will operate CCTV in accordance with:

- UK GDPR;
- Data Protection Act 2018;
- Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice, where applicable;
- Freedom of Information Act 2000, where relevant;
- Human Rights Act 1998;
- ICO guidance on video surveillance;
- the Council's data protection, information governance and records retention policies.

4. Data controller

Haslemere Town Council is the data controller for personal data captured by its CCTV systems. The Council determines the purposes for which CCTV is used and is responsible for ensuring that the system is lawful, necessary, proportionate, secure and properly managed.

5. Purposes of CCTV

CCTV may be used only for the following purposes:

- prevention and detection of crime;
- protection of Council property, premises, facilities and assets;
- public safety;
- safety of staff, councillors, contractors, volunteers and visitors;
- investigation of incidents affecting Council premises, land, assets or services;
- assisting law enforcement agencies where lawful, necessary and proportionate;
- supporting insurance, legal or complaint investigations where lawful and necessary.

CCTV must not be used for general monitoring of residents, visitors or staff, or for any purpose incompatible with this policy.

6. Lawful basis for processing

The Council's usual lawful basis for processing CCTV footage is that it 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.

In some circumstances, CCTV footage may also be processed where necessary:

- to comply with a legal obligation;
- for the establishment, exercise or defence of legal claims;
- to protect the vital interests of an individual in an emergency.

Where CCTV footage includes suspected criminal activity, criminal offence data or special category data, it will be handled in accordance with the Data Protection Act 2018 and the Council's appropriate policy document where required.

7. Data protection principles

The Council will ensure that CCTV footage is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;

- adequate, relevant and limited to what is necessary;
- accurate, where applicable;
- kept for no longer than necessary;
- processed securely;
- managed in a way that demonstrates accountability.

8. Camera locations and coverage

CCTV cameras will be positioned only where necessary and proportionate for the purposes set out in this policy.

The Council will maintain a CCTV Asset Register, recording:

- camera location;
- area covered;
- purpose of camera;
- whether footage is recorded or live-view only;
- retention period;
- whether audio or analytics are used;
- date of last review.

Cameras must not be positioned to unnecessarily capture private property, private gardens, neighbouring premises, areas where individuals have a high expectation of privacy, or areas unrelated to the Council's stated purposes.

Privacy masking or repositioning must be used where appropriate.

9. Data Protection Impact Assessment

The Council will complete and maintain a Data Protection Impact Assessment for its CCTV system.

A new or updated DPIA must be completed before:

- installing new cameras;
- relocating cameras;
- extending camera coverage;
- introducing remote access;
- changing retention periods;
- introducing audio recording;
- introducing facial recognition, ANPR, biometric capability or analytics;
- using CCTV for a new purpose.

The DPIA must assess necessity, proportionality, privacy risks and mitigating safeguards.

10. Signage and privacy information

The Council will display clear and visible signage at locations where CCTV operates.

Signage should state:

- that CCTV is in operation;
- the purpose of the surveillance;
- that Haslemere Town Council is the data controller;
- how to contact the Council;

The Council will publish a CCTV privacy notice on its website and make a copy available on request.

11. Access to CCTV footage

Access to CCTV footage is restricted to authorised officers only.

Authorised access may include:

- the Town Clerk;
- Deputy Clerk or nominated senior officer;
- designated system administrator;
- DPO, where required for compliance review;
- approved contractor, where necessary for maintenance and subject to appropriate safeguards.

Councillors do not have routine access to CCTV footage by virtue of office.

All access, viewing, searching, downloading, exporting, disclosure and deletion must be recorded in the CCTV Access and Disclosure Log.

12. Staff monitoring

CCTV is not installed for routine monitoring of staff conduct or performance.

Footage may be reviewed where necessary to investigate a specific incident, complaint, health and safety matter, security concern, disciplinary matter or legal issue. Any such use must be necessary, proportionate, authorised and recorded.

13. Disclosure of CCTV footage

CCTV footage will not be disclosed to third parties unless there is a lawful basis and the disclosure is necessary and proportionate.

Disclosure may be made to:

- police or law enforcement agencies;
- prosecution agencies;
- courts or tribunals;
- insurers;
- legal advisers;
- regulatory bodies;
- individuals exercising data protection rights, subject to third-party privacy considerations.

Requests should normally be made in writing and recorded. The Council may refuse or restrict disclosure where release would be unlawful, excessive, prejudicial to an investigation, or unfair to third parties.

14. Disclosure to the police

Police requests should normally be made using the police force's data protection request form or equivalent written request.

Before disclosure, the Council should record:

- requesting officer and force;
- crime or incident reference, where available;
- footage requested;
- purpose of request;
- lawful basis or exemption relied on;
- authorising officer;
- method of secure transfer;
- date and time of disclosure.

Where there is an emergency or immediate risk to life or safety, footage may be disclosed urgently, with written records completed as soon as practicable.

15. Disclosure to media

CCTV footage will not normally be released directly to the press, media or social media.
Any proposed release to the media must be exceptional, lawful, necessary, proportionate and approved by the Town Clerk following DPO advice. Where the purpose is to assist identification of a suspect, witness or victim, disclosure should normally be managed by the police.
Images of other individuals must be blurred or otherwise protected unless disclosure is lawful and necessary.

16. Data subject rights (Subject Access Request SAR)

Individuals have rights in relation to their personal data, including the right to request access to CCTV footage showing them.
Requests do not have to be made on the Council's form. They may be made verbally or in writing. However, the Council may ask for sufficient information to identify the requester and locate the footage, including:

- date;
- approximate time;
- location;
- description of the requester;
- proof of identity;
- recent photograph, where necessary to identify the requester in the footage.

The Council will respond to requests without undue delay and normally within one calendar month.
The Council may refuse, restrict or redact footage where disclosure would adversely affect the rights and freedoms of others, prejudice crime prevention or detection, or where another legal exemption applies.

17. Fees

The Council will not charge a standard fee for responding to a data subject access request.
A fee may only be charged where permitted by data protection legislation, for example where a request is manifestly unfounded or excessive, or where a fee is permitted for additional copies.

18. Retention and deletion

Routine CCTV footage will normally be retained for no longer than **30 days**, unless a shorter period is specified in Schedule 1 or a longer period is justified.

Footage may be retained for longer where necessary for:

- police investigation;
- legal proceedings;
- insurance claims;
- complaint investigation;
- health and safety investigation;
- disciplinary investigation;
- protection of Council property or assets.

Footage retained beyond the standard retention period must be recorded, reviewed periodically and securely deleted when no longer required.

19. Security

The Council will protect CCTV footage using appropriate technical and organisational measures, including:

- restricted user access;
- unique user accounts where available;
- strong passwords;
- multi-factor authentication for remote access where available;
- secure storage of recordings;
- secure export methods;
- encryption or password protection for transferred footage;
- audit logs;
- physical security for equipment;
- secure deletion;
- contractual controls for suppliers.

CCTV footage must not be stored on personal devices, personal cloud accounts, unencrypted USB drives or personal email accounts.

20. Contractors and processors

Where a contractor or supplier can access CCTV footage or systems, the Council must ensure appropriate written terms are in place.

Contracts must require the contractor to:

- act only on the Council's instructions;
- maintain confidentiality;
- protect footage securely;
- restrict access to authorised personnel;
- report breaches promptly;
- assist with data subject rights requests;
- delete or return data when no longer required.

21. Personal data breaches

Any loss, unauthorised access, unauthorised disclosure, accidental deletion or inappropriate use of CCTV footage must be reported immediately to the Town Clerk and DPO.

The Council will assess whether the breach must be reported to the ICO and/or affected individuals.

22. Complaints

Complaints about the Council's use of CCTV should be made to the Town Clerk in the first instance.

Individuals also have the right to complain to the Information Commissioner's Office if they are dissatisfied with how the Council has handled their personal data.

23. Training

Officers with access to CCTV systems or footage must receive appropriate training on:

- this policy;
- data protection principles;
- access controls;
- disclosure procedures;
- subject access requests;
- retention and deletion;
- incident reporting.

24. Monitoring and review

This policy will be reviewed annually, or sooner if:

- legislation or ICO guidance changes;
- cameras are installed, moved or removed;
- the system is upgraded;
- a data breach occurs;
- a complaint identifies a policy weakness;
- the DPIA identifies new risks.