South Molton Town Council

CCTV Policy

Adopted: 11th March 2020

This Policy should be read with reference to the General Data Protection Regulation 2018 (GDPR), the Data Protection Act 2018 (DPA), the Freedom of Information Act 2000 (FOIA), the Protection of Freedoms Act 2012 (PFA), the Human Rights Act 1998 (HRA), the Regulatory and Investigatory Powers Act 2000 (RIPA), the Secretary of State's Surveillance Camera Code of Practice (SC code), and the Information Commissioner's Office (ICO) CCTV Code of Practice.

1. Background & Introduction

The processing of personal data captured by CCTV systems (including images identifying individuals) is governed by the Protection of Freedoms Act 2012 and the Data Protection Act 2018. The Information Commissioner's Office (ICO) has issued a Code of Practice on compliance with legal obligations. The use of CCTV is covered by the Acts, regardless of the number of cameras or how sophisticated the equipment is. South Molton Town Council adheres to the ICO's Code of Practice.

South Molton Town Council is committed to informing the public, its staff and service users about the presence of and operation of CCTV. This Policy is available on the Town Council's website so that all stakeholders are clear about how CCTV is utilised by the Town Council.

Access to personal information recorded through CCTV cameras **is restricted solely to the Data Protection Officer or other nominated person appointed by South Molton Town Council.**

2. Objectives

This CCTV Policy explains how South Molton Town Council will operate its CCTV equipment and comply with the current legislation.

South Molton Town Council uses CCTV equipment to deter crime, combat vandalism and theft, and to provide a safer, more secure environment for the public, its staff and service users. Essentially it is used for:

- The prevention, investigation and detection of crime.
- The apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings).

- Safeguarding the public and staff.
- Monitoring the security of the site.
- To protect members of the public and public property.

South Molton Town Council does not use the CCTV system for covert monitoring.

3. Location

Cameras will be located in those areas where it has been identified there is a need and where other solutions are ineffective. The CCTV system is used solely for the purposes identified and is not used to routinely monitor the public, staff, or service users conduct. Cameras will not be used in areas subject to a heightened expectation of privacy e.g. changing rooms or toilets. Signage will alert individuals to the use of CCTV.

Cameras will not focus on private homes, gardens or other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Recordings will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. Tapes will never be released to the media for purposes of entertainment.

4. Maintenance

The CCTV system is maintained by South Molton Town Council and includes periodic maintenance inspections.

South Molton Town Council is responsible for ensuring:

- Compliance with its responsibilities in relation to guidance on the location of cameras.
- The Data Protection Officer is trained in the use of the equipment.
- Suitable maintenance and servicing is undertaken to make sure that clear images are recorded.
- Date and time references on any captured footage are accurate.

5. Identification

The Town Council will ensure that prominent signs are in place where any cameras are sited.

The signs will:

- Be clearly visible and legible.
- Be an appropriate size depending on context.
- Contain details of the organisation operating the scheme, the purpose for using CCTV and who to contact about the scheme.

6. Audio Recording

South Molton Town Council's CCTV cameras record visual images or property only and do not record sound.

7. Administration

South Molton Town Council is the Data Controller and the Data Protection Officer has responsibility for the control of images and deciding how the CCTV system is used. The Council is registered with the Information Commissioner's Office - Registration Number Z714506X.

Only the Data Protection Officer will have access to images and is aware of the procedures that need to be followed when accessing the recorded images. The Data Protection Officer is trained and is aware of responsibilities under the CCTV Code of Practice: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

Access to recorded images is restricted to the Data Protection Officer and recordings will be accessed as prescribed by the Council in the event of an incident.

Access to the medium on which the images are recorded is documented. All employees are aware of the restrictions in relation to access and security, and disclosure of, recorded images.

8. Image storage, viewing and retention

Recorded images will be stored in a secure fashion that will not permit unauthorised access and that will ensure the integrity of the image and will allow specific times and dates to be identified.

South Molton Town Council reserves the right to use images captured on CCTV where there is activity that cannot be expected to be ignored such as criminal activity or anti social behaviour which puts others and or property at risk . The Data Protection Officer will retain images for evidential purposes in a locked area. Where images are retained, the Data Protection Officer will ensure that records of the following are kept:

- The reason for their retention.
- Where they are kept.
- Use made of the images
- The date of their erasure.

The Town Council will ensure that images are not retained for longer than 31 days unless they are required for evidential purposes. Once the retention period has expired, images will be erased.

9. Disclosure

Disclosure of the recorded images to third parties can only be authorised by the Data Controller. Disclosure will only be granted:

- If there is an overriding legal obligation (e.g. information access rights).
- If it is consistent with the purpose for which the system was established.

All requests for access or for disclosure are recorded. If access or disclosure is denied, the reason is documented.

N.B Disclosure may be authorised to law enforcement agencies, even if a system was not established to prevent or detect crime, if withholding it would prejudice the prevention or detection of crime.

10. Subject Access Requests

Individuals whose images are recorded have a right to view images of themselves and, unless they agree otherwise, to be provided with a copy of the images. If the Town Council receives a Subject Access Request under the General Data Protection Regulations 2018 it must comply with the request within one month. The Council may only charge a fee for the provision of a copy of images. If the Council receives a request under the Freedom of Information Act 2000 it must comply with requests within 20 working days of receiving the request.

Generally, if the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data and its disclosure is unlikely as a Freedom of Information request.

Those requesting access must provide enough detail to allow the operator to identify that they are the subject of the images, and for the operator to locate the images on the system. Requests for access should be addressed to the Data Controller.

We are entitled to deny access to information under certain cases under the Data Protection Act, specifically, where the information may be held for:

- The prevention and detection of crime.
- The apprehension and prosecution of offenders.

In any allegations of crime, we will only provide footage to the police and, in any request in respect of a road traffic collision, any footage will only be released to the police or relevant insurance company.

11. Monitoring and evaluation

South Molton Town Council undertakes regular audits to ensure that the use of CCTV continues to be justified. The audit includes a review of:

- The location.
- Its stated purpose.
- The images recorded.
- Retention period.
- Deletion.

12. Period of Review

The efficacy of this Policy will be reviewed annually by South Molton Town Council.

[END]

Appendix 1

Guiding Principles

System operators should adopt the following 12 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 use 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.

[END]

Appendix 2

Privacy Impact Assessment – ATM CCTV

1 Privacy Impact Assessment

1.1	What is the aim of the surveillance system?	To detect, deter and prevent crime and to improve public safety and public reassurance.
1.2	What organisations will have access to CCTV images? Who will take legal responsibility under the Data Protection Act?	South Molton Town Council (SMTC) and Devon and Cornwall Police are the main users of the CCTV system. SMTC is the Data Controller at the point of images being recorded, however, if any images are released to any of the authorised organisations, then the legal responsibility will be transferred to that organisation in relation to the images that have been released.
1.3	What and who will benefit from the system?	ATM users and the general public will benefit from improved public safety, and reductions in crime.
1.4	Can CCTV realistically deliver these benefits?	Yes, the installation of a CCTV camera was a condition imposed by the police
1.5	Why is a Privacy Impact Assessment required?	The surveillance system collects personal data (CCTV Data).

2 Information Flow

2.1	How is information collected?	Through the use of an overt public space CCTV camera. Cameras record 24 hours per day.
2.2	Where are the real time images from the camera displayed?	No real time images are displayed.
2.3	Who has operational access?	Only One SMTC Employee has access. Devon and Cornwall Police can be granted use of cameras in the control room under the Regulation of Investigatory Powers Act. This is strictly controlled and only authorised by the rank of Superintendent or above.

Privacy Impact Assessment – ATM CCTV

2.4	How are the images recorded?	Digital Storage Media/ Hard Drive
2.5	Where are the recorded images stored?	Town Hall Market Office
2.6	How is information stored?	A digital recording and data management system is in place which covers all data collected by the CCTV surveillance system.
2.7	What measures are in place to control access to the area in which the recorded images are stored?	Secure access to the CCTV control room.
2.8	How is information used?	• Information is used to monitor public safety and prevent and detect crimes. • Evidence is provided for investigation and enforcement. • Individuals can request copies of CCTV data which contains their personal information. • Disclosure of data is covered by internal processes in full compliance with relevant legislation and codes of practice.
2.9	How is access gained to the recorded images?	Data management control levels established on system. Password controls on system. Hard copy requests for images required.
2.10	How long are the images retained?	Approx 31 Days by movement only
2.11	How is information deleted	The data management system automatically deletes information after 31 days unless it has been saved in the systems evidence locker.
2.12	When data is downloaded or copied for release to a third party how is information recorded?	DVD or Hard Drive
2.13	What processes are in place to ensure that data protection responsibilities are understood by persons receiving the data?	Each request for data must be requested via a signed data release form. In case of the Police this is authorised by a person at the rank of Sergeant or above.
2.14	What precautions are in place to ensure that data will continue to be collected in the event of a failure of power?	No Data Collected in event of Power Cut

3. Risks

3.1	Have you identified solutions to address any risks identified?	The system is operated in line with relevant legislation and codes of practice.
3.2	Is the data shared with other organisations?	Yes for investigation and enforcement.
3.3	Is the system operated in full compliance with (i) DPA requirements (ii) ICO codes of practice (iii) SCC codes of practice (iv) Human Rights Act?	Yes
3.4	Do you have procedures in place to manage risks associated with the use of CCTV cameras?	Yes

4. Privacy

4.1	Can less privacy intrusive solutions achieve the same objectives?	No, the system was installed on the advice of the police.
4.2	Are images of identifiable individuals required or could the scheme use other technology not capable of identifying individuals?	The system must be capable of identifying individuals, as footage from the system will be used in both criminal and civil court cases. If the system did not have this capability it would not be fit for purpose.
4.3	Will the particular equipment/ system of work being considered deliver the desired benefits now and remain suitable in the future?	Yes, SMTC will continue to operate the system on a 24-hour basis in line with all relevant legislation.
4.4	What future demands may arise for wider use of images and how will you address these?	Legislation can and does change. We will comply with all future regulations placed upon us.
4.5	What are the views of those under surveillance?	ATM users are happy to be in an area that is monitored by CCTV cameras.

5 Human Rights Act

5.1	What could we do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed? Is the system established on a proper legal basis and operated in accordance with the law?	The system is specifically to deter crime and make ATM service users feel safer. The system has been established on a proper and legal basis and we comply with the Data Protection Act, Human Rights Act and Regulations of Investigatory Powers Act.
5.2	Is it necessary to address a pressing need, e.g. public safety, crime prevention or national security?	Yes. The system has been installed at the request of the police in order to deter crime.
5.3	Is it justified in the circumstances?	Yes.
5.4	Is it proportionate to the problem that it is designed to deal with?	Yes. CCTV is used to detect crime and complies with the current legislation

[END]