



St Ives Town Council

CCTV Policy

Policy / File Status

Version	0.1	Approving Body	Full Council
Date	06.01.25	Date of Approval	13.02.25
Responsible Officer	Town Clerk	Minute Reference	C.129
Oversight Committee	F&GP Committee	Review Date	January 2026

Version History

Date	Version	Author/Editor	Comments
20.12.24	0.1	Town Clerk	New policy drafted and introduced following the transfer of CCTV management from Cornwall Council

Review Record

Date	Type of Review Conducted	Summary of Actions Taken or Decisions Made	Completed By

Contents

Section	Title	Page
1.0	Introduction	1
2.0	Objectives of the CCTV systems	5
3.0	Key Principles	5
4.0	Ownership and Management of CCTV	5
5.0	Management and Operation of CCTV systems	6
6.0	Installation and Privacy	8
7.0	Assessment of CCTV systems and National Code of Practice	9
8.0	Maintenance of CCTV systems	9
9.0	Management and Operation of CCTV systems and Recorded data	9
10.0	Surveillance Camera National Code of Practice	10
11.0	Protection of Freedoms Act 2012	11
12.0	GDPR and Subject Access Requests – Request for Personal Data	11
13.0	The Regulation of Investigatory Powers Act 2000 (RIPA)	11
14.0	Information Commissioner’s Office	11
15.0	Security, Complaints and Breaches of this Policy	12

1. Introduction

- 1.1 St Ives Town Council own, operate and manage the data of closed circuit television (CCTV) systems that survey public areas, council buildings and associated land throughout the parish.
- 1.2 Public Space CCTV cameras are located in public areas around the town centre, primarily on the highway. These cameras are monitored throughout the year in real time recording. Recordings are retained for 31 days and thereafter are automatically erased, unless saved to hard drive. Saved data are retained for one calendar year. These cameras are called the **town centre CCTV system**. They are monitored in a local control room on the Council's behalf by a contractor, operating in accordance with the Council's policies and procedures. The contractors are also responsible for monitoring and managing cameras for Hayle and Penzance Town Councils in the same control room facilities under their own policies and procedures. Queries about systems in other towns should be directed to the relevant town council.
- 1.3 Our control room facilities are equipped for the future use of a police radio. Local police have access to live and post images from the cameras so we can quickly notify them if there is an incident. Recordings are retained for 31 days and thereafter are automatically erased, unless saved to hard drive. Saved data are retained for one calendar year.
- 1.4 There are many other CCTV systems within the town and parish of St Ives, owned and operated by private members of the public, the Police, businesses, Cornwall Council and the Town Council.
- 1.5 Corporate Council CCTV cameras are located around key areas of land and buildings and are owned and / or managed by the Council. These include the Guildhall and the Cornerstone library, outside public conveniences, and parks and gardens, including Palemon Best park and Trewyn Gardens. Some of these cameras are monitored 24/7/365 in real time recording. On some sites recording is done locally. Recordings are retained for 31 days and thereafter are automatically erased unless saved to hard drive. Saved data are retained for one calendar year.
- 1.6 Body Worn Video is used by the Civil Parking Enforcement multi-skilled enforcement officers while enforcing the town PSPO. Officers are employed by Cornwall Council and deliver some services on the Town Council's behalf. These cameras record at the sole discretion of that service in line with their policies, procedures and training. Once activated, the camera records visual images and audio in real time until the officer stops the recording. Recordings are retained in line with Cornwall Council's data retention policies.
- 1.7 All Council owned CCTV has signage stating its purpose and contact details.
- 1.8 This policy applies to all CCTV systems owned or operated on behalf of St Ives Town Council, in public areas, land and corporate site areas.
- 1.9 The policy is to ensure the Council's CCTV systems are managed effectively, efficiently and lawfully. For Town Centre CCTV, there are operational and

contractual procedures in place, setting out how the contractor manages the system in the control room.

- 1.10 St Ives Town Council operates Town Centre CCTV in partnership with the Town Councils of Penzance and Hayle, Devon and Cornwall Police, Cornwall Council and other stakeholders.
- 1.11 The principles and governance for the deployment of Body Worn Video (BWV) are owned and governed by Cornwall Council and operate solely in accordance with their policies and practices.
- 1.12 Corporate CCTV is operated internally by St Ives Town Council, in accordance with this policy.

2.0 Objectives of the CCTV systems

2.1 The objectives of the Council's CCTV systems are as follows:

- To reduce the fear of crime promoting a feeling of safety.
- To deter crime, detect crime and provide evidence of offences
- To deter and assist in the prevention of anti-social behaviour.
- To identify and or monitor risk and vulnerability.
- To assist in providing the safety and security of employees, members of the public, contractors, building and assets.
- To enhance community safety, thereby assisting in developing the economic well-being of St Ives parish and encouraging greater use of public open spaces, facilities and amenities.
- To detect and prevent environmental issues
- To assist the Council in enforcement and regulatory functions.
- To assist in the management of Council premises.

3.0 Principles

- 3.1 Individual CCTV systems shall be operated fairly, lawfully and in accordance with this policy.
- 3.2 Each CCTV system is operated to ensure the privacy of the individual and their human rights. The Human Rights Act 1998 gives effect to the rights set out in the European Convention on human rights. Some of these rights are absolute, whilst others are qualified, where it is permissible for the state to interfere so long as it is in *pursuit of a legitimate aim* and proportionate.
- 3.3 The application of this policy will ensure that CCTV systems are installed and operated in such a manner as to preserve the right to respect for private and family life conferred by article eight (8) of the European Convention on Human Rights. Adherence to the Council's policy will ensure correct handling of recorded images, which will avoid breaches of article six (6), the right to a fair hearing. The public interest in the operation of CCTV systems shall be maintained through the security and integrity of operational and procedural systems.

4.0 Ownership and Management of CCTV systems

- 4.1 St Ives Town Council own, manage and are responsible for the compliance with this policy, ensuring the rights and interests of the public and of individuals are maintained.
- 4.2 The day-to-day operation of the systems is the responsibility of the Council and or its providers contracted by the Council for such purpose. Relevant legislation and guidance which inform the policy are as follows:

Freedom of Information Act 2000 (FOIA)
GDPR and Data Protection Act 2018
the Human Rights Act 1998 (HRA)
the Surveillance Camera code of practice issued under the protection of Freedoms Act 2012, as updated by Government in 2021
Information Commissioner's Office – video surveillance guidance (2022)

- 4.3 In compliance with the Information Commissioners Office (ICO) guidance, all systems should be properly signed to inform members of the public who to contact about the management and purposes of the system.

5.0 Management and Operation of CCTV systems

- 5.1 Only authorised, Security Industry Authority licenced (SIA), Non-Police Personnel Vetting Level 1 (NPPV1) and Disclosure Barring Service (DBS) and signed off trained persons are to operate CCTV systems and associated equipment. Refresher annual training for operators and supervisors with applicable re-applications for SIA Licence, Police Vetting and DBS checks.
- 5.2 The operators of the system will be required to adhere to this policy at all times. The Council and Council contracted staff will be subject to their employer's disciplinary procedures in the event of a breach of this code and/or associated operational manuals and procedures.
- 5.3 Camera and associated equipment usage shall concur with the purposes and key objectives of the CCTV scheme and shall comply with this policy.
- 5.4 Only Council members of staff or contracted staff with responsibility for using the equipment shall have access to operating controls. Operators of the CCTV system must act with the utmost integrity and take personal responsibility.
- 5.5 A requirement of confidentiality will be enforced during and (where necessary) after termination of employment. A CCTV confidentiality form must be signed and annual renewal for individuals deployed within the CCTV Control Room or any other monitoring areas.
- 5.6 CCTV systems are to be audited annually to ensure the requirements and objectives to operate the system still remains. This applies also to the requirement of collecting and retaining personal data ensuring other legal requirements, policies and standards are complied with in practice. This is in accordance with the Information Commissioner's (ICO) CCTV guidance (2022), the Secretary of State's surveillance camera Code of Practice (2013 and amended 2021).

- 5.7 Security of the CCTV control room and recorded material. CCTV monitoring and control equipment, and access to recorded images, is to be restricted and only used for the purposes stated in or referred to in this policy.
- 5.8 Recorded images are to be kept securely at all times and live and recorded images are only to be viewed and reviewed to meet the purposes of each system. Access to the Council's CCTV equipment and control room(s) is to be restricted to those managing, operating or maintaining the CCTV Control Room and its systems or other authorised personnel, strictly in accordance with this policy and the operational manual.
- 5.9 A log is to be maintained of all visitors to the control room(s) recording the visitors' confirmation that they will maintain the confidentiality of control room operation along with personal data and the time of arrival and departure. Visitors are NOT permitted to use the systems.
- 5.10 Members of the broadcast and print media will not be permitted access to the control rooms and CCTV equipment unless authorised in writing by the Town Council and agreed with the contracted operator (in the case of externally managed systems).
- 5.11 The system operators will hold primary responsibility for ensuring there is no breach of security and that this policy is complied with at all times. They will have day-to-day responsibility for the management of the control room and for enforcing operational and disciplinary codes.
- 5.12 The designated systems operator will ensure that any serious breach of this policy is duly notified in accordance with the Council's Data Protection policies and procedures. Staff will perform their duties ensuring strict compliance with this code, agreed operational procedures and with due regard to confidentiality.
- 5.13 Any breaches will be subject to investigation and possible disciplinary action in accordance with the Council or its contractor's procedures.
- 5.14 Police use of the CCTV systems applies equally to the police and other statutory investigation agencies use of the CCTV systems.
- 5.15 Where a police operation requires a RIPA authority, the authorisation for such surveillance must be produced before the CCTV equipment is used and the authorisations must be retained securely.
- 5.16 Access to the control room will be permitted to duly authorised Police Officer(s) for the purposes of taking written statements, accessing authorised data manually where this cannot be transferred through a secure electronic platform and use of the CCTV equipment including partnership working.
- 5.17 Police use of the CCTV system, including both the review of recorded as well as viewing live images, is to be strictly controlled including logging.
- 5.18 No police officer or member of police staff is to use the CCTV equipment without permission and unless there is a clear operational requirement to do so.
- 5.19 Details of each and every use is to be recorded on the applicable police log or in a book kept for the purpose, both at the time of release and recovery of the system.

- 5.20 Any remote control and recording of cameras will strictly adhere to this policy and special management and data protection policies and arrangements in place.

6.0 Installation and Privacy

- 6.1 All CCTV images must be adequate for the purpose for which they are collected, and surveillance cameras should be sited in such a way that they only survey those areas that are intended to be viewed by the equipment. Siting of equipment and cameras should always include an assessment of the impact on privacy. However, where privacy intrusion is identified following installation, steps must be taken to remove/minimise intrusion.
- 6.2 Permanent and or relocatable cameras should be sited and images captured/restricted to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, such as individuals' private property.
- 6.3 The cameras must be sited and the system must have the necessary technical specification to ensure that images are of a suitable quality for the purpose for which the system was installed.
- 6.4 Prior to installation of a new system or significant addition to an existing system, the Council shall consult with stakeholders and the community.
- 6.5 The assessment for installation should aim to establish clear Operational Requirements for the camera(s) and or systems and take into account the benefits gained.
- 6.6 The assessment for installation should also demonstrate whether or not other or better solutions exist and what effect it may have on individuals and their privacy.
- 6.7 The Council shall consider whether it is justifiable in the circumstances and a proportionate response to the issue being addressed. From time to time relocatable or transportable cameras may be installed temporarily. The use of such cameras and the data produced by their use will always accord with the objectives of CCTV and this policy.
- 6.8 Installation must meet the requirements of the Defence Science and Technology Laboratory guidance [Digital Imaging CCTV and Video based evidence](#). *Procedures and guidance on capturing and recovering images, video and audio including standards for installing CCTV (January 2024)*
- 6.9 Some people regard surveillance cameras as an infringement of personal liberty. Everyone has the right to respect for their private and family life in line with [Data Protection Act 1998](#). Where there is an expectation of privacy, the cameras shall have masking applied. CCTV operators shall be trained on how best to manage operating cameras eliminating or reducing intrusion of privacy.

7.0 Assessment of CCTV systems and Code of Practice

- 7.1 The Council will ensure that all CCTV systems under its ownership and control (and this policy) shall be evaluated from time to time to assess crime, anti-social

behaviour, security and safety impact on neighbouring areas without CCTV, the views of the public and the operation of this policy.

- 7.2 The Council officer with the day-to-day responsibility for CCTV (CCTV Single Point of Contact) will monitor the operation of CCTV systems and the implementation of this policy. They will recommend any element for review or amendment in response to legislative and governance changes or in response to consultation or other external events.

8.0 Maintenance of CCTV equipment

- 8.1 CCTV systems and associated equipment are to be repaired, maintained and kept in full working order so as to meet the Operational Requirements. A budget, sufficient to support this requirement shall be maintained and reviewed annually. The maintenance of the town centre equipment is currently undertaken under a contract with Enerveo Ltd. Any issues relating to the condition of the cameras and associated hardware, including vandalism or damage should be reported to the Council at enquiries@stives-tc.gov.uk.

9.0 Management and Operation of CCTV systems and Recorded data

- 9.1 Management of recorded data/material, including still image prints, will only be used for the purposes defined in this policy and access restricted.
- 9.2 Recorded material will under no circumstances be sold or used for commercial purposes or for the provision of entertainment.
- 9.3 The Council may use recorded images for training purposes and to promote the effectiveness of its CCTV systems.
- 9.4 No more images and information shall be stored other than that which is stringently required for the stated purpose of a surveillance camera system.
- 9.5 Such images and information shall be deleted once their purposes have been discharged. This is typically 31 days, though this may vary from scheme to scheme. Retained data is held for one calendar year and should be then deleted.
- 9.6 Showing the recorded images to members of the public will only be permissible in accordance with the law, either in compliance with the prerequisites of the police in connection with investigation of crime, or any other circumstances provided by the law. Access to recorded images by the police, other statutory investigation agencies or officers of the court is permissible under the [Data Protection Act 1998](#), [Police and Criminal Evidence Act \(PACE\) 1984](#) and the [Criminal Procedures and Investigations Act 1996](#).

Control Room and systems.

The data and information transmitted and recorded in the town centre CCTV Control Room is confidential, classified and sometimes sensitive. Access to Data security and ethical considerations are paramount to St Ives Town Council. Our CCTV policy complies with relevant guidance and law, including the Human Rights Act, the Equality Act, the Data Protection Act and UK GDPR, and the Data Ethics Framework. Details of the relevant legislation and statutory guidance are summarised below.

10. Surveillance Camera National Code of Practice

10.1 Under a national [Surveillance Camera Code of Practice](#), updated in 2021 and re-issued by the secretary of state, camera operators are required to follow 12 guiding principles as follows:

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 user 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.

11. Protection of the Freedoms Act 2012

11.1 The CCTV Control Room is strictly controlled and with risks managed at all times to ensure compliance with the Data Protection Act and UK GDPR is not breached.

12. GDPR and Subject Access Requests – Request for Personal Data

12.1 *St Ives Town Council is the Data Controller for all surveillance in the CCTV.*

12.2 Under the [Data Protection Act 1998](#) individuals are permitted to have copies of any personal data held by the Council, including recorded CCTV images. The process for obtaining this is the submission of a subject access request. More information on subject access requests is published by the Information Commissioner's Office and can be viewed [HERE](#).

12.3 The Council may deny access to information where the act allows, particularly where it may prejudice, prevention and detection of crime or the apprehension, prosecution of offenders or the exercise of the Council's statutory functions.

12.4 Subject Access Requests (SAR) for CCTV images should be sent to:

**The Town Clerk
St Ives Town Council
The Guildhall
Street an Pol
St Ives
CORNWALL
TR26 2DS
enquiries@stives-tc.gov.uk**

13.0 The [Regulation of Investigatory Powers Act 2000](#) (RIPA 2000)

13.1 Council CCTV systems shall be managed and operated in accordance with this Act.

13.2 Regulation of Investigatory Powers Act 2000 deals with the covert surveillance activities of public authorities. Any covert use of CCTV systems by or on behalf of a public authority and with the authority's knowledge immediately places such use within the bounds of the RIPA Act. The requirements of RIPA shall be complied with at all times.

14.0 Information Commissioner's Office (ICO)

14.1 The ICO code of practice provides guidance and advice for CCTV users on how to comply with the Data Protection Act and also includes a simple checklist for users of very limited CCTV systems where the full provisions of the code would be too detailed.

14.2 St Ives Town Council's CCTV system is registered with the Information Commissioners Office (ICO) for the use of CCTV systems in accordance with the Data Protection Act 1998 and will ensure that the principles of the Data Protection Act are adhered to.

15.0 Security, Complaints and Breaches of this Policy

- 15.1 Complaints and breaches of the policy including those of security will be dealt with in accordance with the Council's or relevant partner's complaints procedures. The Council has a corporate complaints procedure webpage to enable users of Council services to make a complaint. A copy of the complaints policy can be found on our website [HERE](#)