



PADSTOW TOWN COUNCIL

Procedure For Accessing, Disclosing And Handling Data Retrieved From The CCTV System

POLICY/PROTOCOL/PROCEDURE			
Version	Version 1	Comments	
Approval Date	25 July 2023	Responsible Officer	Town Clerk
Committee	LTOS	Approval by	Full Council

VERSION HISTORY		
Date	Version	Comments
18 July 2023	JULY 2023 draft	New Policy drafted.
25 July 2023	Version 1	Approved by FC 25 July 2023

REVIEW RECORD		
Date Review initiated	Review undertaken by i.e. officer/ Cttee/Council	Summary of any recommended updates/changes to be made

1. Scope

- 1.1 The purpose of this procedure is to ensure that data from the CCTV System is accessed, disclosed and handled in a lawful, consistent, secure and confidential manner. It should be read and used in conjunction with the Padstow Town Council CCTV Policy.

2. Accessing Data

- 2.1 Recording equipment will be kept in a secure place and only authorised access to such equipment will be permitted.
- 2.2 Access to recorded data will be restricted to specified system users. System users are responsible for ensuring any individual security information or passwords remain confidential to them.
- 2.3 When accessing data, system users must have regard for where the screening is being conducted and ensure it cannot be observed by unintended persons including employees or Councillors of Padstow Town Council where viewing the data would not be necessary to the observer's role.

3. Applications For Disclosure Of Images

- 3.1 All requests for CCTV data from both individual data subjects and third parties must be submitted in writing via an Application For CCTV Data Access form. Forms are available on the Town Council's website at <https://padstow-tc.gov.uk/your-council/council-policies-procedures/> or from the Town Council Offices, Station House, Station Road, Padstow, Cornwall PL28 8DA.
- 3.2 Application forms will be considered from the following third parties under specific circumstances:
 - i) Data Subjects – a subject access request (SAR);
 - ii) Law enforcement agencies - where the data would assist with a specific criminal enquiry;
 - iii) Prosecution agencies - where the data would assist in the prosecution of anti-social behaviour and criminal activity; and
 - iv) Authorised investigators - such as insurance companies investigating claims in relation to anti-social behaviour and criminal activity.
- 3.3 Upon receipt of a completed application from one of the above and on the authorisation of the Town Clerk, or in her absence the Assistant Town Clerk/Assistant RFO, a system user will access and view the relevant recordings.
- 3.4 The Town Council is not obliged to comply with the request if disclosing the data would be likely to:
 - i) Prejudice the prevention and detection of crime;
 - ii) Prejudice the apprehension and prosecution of offenders; or

iii) Contravene the data protection rights of any third party in the footage whose identity cannot be protected unless it is satisfied that the individual has provided their express consent to the disclosure or it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

3.5 In order to locate images on the system, sufficient detail must be provided in order to allow the relevant images to be located and the data subject to be identified. The CCTV system stores data for a maximum of 30 days before it is automatically deleted by the digital management system. 30 days is considered to be sufficient for subject access requests and investigatory requests to be made.

3.6 Where a request for access is received from a data subject (a Subject Access Request), the data subject will be required to establish their identity by supplying the following documents:

One of the following:

- Valid photo driving licence
- Full valid current passport
- Recent passport sized photograph

And **two** of the following:

- Birth certificate or Adoption certificate
- Valid driving licence
- Utility Bill (gas, electricity, water, or telephone) in the applicant's name for the last quarter
- Medical card
- Bank, Building Society or Credit Card statement in the applicant's name for the last quarter
- Council Tax bill/demand in the applicant's name for the last quarter

At least one document must show their current address and at least one must show their date of birth.

4. Disclosure Of Images

4.1 Receipt of an Application For CCTV Data Access form will be acknowledged as soon as possible, typically within 5 working days. Requestors will be given the opportunity to view the data, or reasons why it cannot be provided, within 20 working days of Padstow Town Council receiving the request.

4.2 If the incident requested is found, the system user will download the recording to an encrypted USB device specifically for this purpose. The system user will then clearly label the USB and place it in the secure lockable evidence location until it can be shared with the requester.

4.3 In the first instance, the offer of an on-site visit to view the data will be made. In these circumstances, the data will be disclosed by an authorised system user in a private space where the screening cannot be observed by unintended

persons including other employees of Padstow Town Council. For SAR viewings, the data subject will be required to bring identification as outlined in 3.6 above.

- 4.4 Where a copy of the footage is requested, a fee of £30 is payable and must be paid prior to its release.
- 4.5 The USB can be collected from the Town Council Offices by the requester at a pre-arranged time. Data being collected in person that is released as an SAR must be collected by the data subject and the data subject will be required to bring identification as outlined in 3.6 above.
- 4.6 If the requester does not wish to collect the data in person, the requester will need to consent to the USB being sent by recorded delivery post. It should be taken to the post office as soon as reasonably practicable and stored in the lockable evidence location until that time. Data being released as an SAR will only be sent to the data subject's current address as provided in their identification evidence as outlined in 3.6 above.
- 4.7 For both methods of releasing data, the encryption password will be sent separately to the USB by a system user either by email or post.
- 4.8 A log of any disclosure made will be maintained itemising the date, time, camera, requestor, reason for the disclosure requested, lawful basis for disclosure, date of decision, name of authoriser, name of system user, method of release, date of release, and name of authorised person actioning the release.
- 4.9 In requesting the disclosure or release of recorded data, the requester accepts full responsibility for its security and management once it has been released from the Town Council. Padstow Town Council shall not be liable regarding any matter arising from the security, management or use of an authorised disclosure of recorded data to any third party.

5. Handling Retrieved Data

- 5.1 Data retrieved from the CCTV system must be stored in the specified lockable evidence location at all times. Data stored in the lockable evidence location may be retained in excess of the Town Council's 30 day retention period under the circumstances outlined in paragraph 4 above, and where there is a requirement to hold the data for longer, for example where the data relates to a major incident involving civil proceedings.
- 5.2 Access to the lockable evidence location will be restricted to authorised employees who have been approved by the Town Clerk, or in her absence the Assistant Town Clerk/Assistant RFO. Employees with authorised access to the lockable evidence location may not necessarily be system users.
- 5.3 Data stored in the secure lockable evidence location will be kept on individual USBs which are encrypted and clearly labelled. A log of evidence stored in the lockable evidence location will be maintained. A separate log of encryption

codes will be maintained and access to the encryption log will be restricted to system users.

- 5.4 The Town Clerk will ensure that evidence retained in the lockable evidence location is reviewed on a quarterly basis and is destroyed when it is no longer necessary to keep.