

# **TORPOINT TOWN COUNCIL**

## **CCTV, BODY-WORN VIDEO AND VEHICLE- BORNE CAMERA POLICY**

**REVIEWED: - September 2026**

**NEXT REVIEW: - September 2027**

**REVIEWING BODY: - Finance and Operations Committee**

## **CONTENTS**

- 1. Introduction**
- 2. Scope of the Policy**
- 3. Purposes of Surveillance**
  - 3.1 CCTV
  - 3.2 Body-Worn Video
  - 3.3 Vehicle-Borne/Dashboard Camera
- 4. Lawful Basis and Data Protection**
- 5. Privacy and Proportionality**
- 6. Data Protection Impact Assessments**
- 7. Signage and Transparency**
- 8. CCTV Operation**
- 9. Body-Worn Video Operation**
- 10. Council Vehicle Dashboard Camera**
- 11. Harvey Street Flats**
- 12. Data Security and Access**
- 13. Retention and Deletion**
- 14. Access to and Disclosure of Images**
- 15. Disclosure to the Media**
- 16. Data Subject Requests**
- 17. Data Breaches**
- 18. Complaints**
- 19. Governance and Responsibilities**
- 20. Training**
- 21. Surveillance System Register**
- 22. Annual Surveillance Review**
- 23. Policy Review**
- 24. Council Contact**
- 25. Sources and Guidance**

### **1. Introduction**

Torpoint Town Council operates closed-circuit television (CCTV), body-worn video (BWV) and vehicle-borne video surveillance systems at specified Council premises and in connection with specified Council activities.

The purpose of these systems is to assist in protecting visitors, staff, members of the public, Council property and facilities, and to support the prevention and investigation of crime, anti-social behaviour, vandalism, health and safety incidents and other matters falling within the Council's legitimate functions.

The Council currently operates CCTV at the following locations:

- Thanckes Park Play Park;
- Thanckes Park Tennis Courts;
- Torpoint Community Hub and Library;
- Benodet Park;
- Harvey Street Flats, subject to the arrangements described in this policy.

The Council also operates body-worn cameras for designated employees and a dashboard/vehicle-borne camera in a Council vehicle.

All surveillance systems operated by the Council will be used in accordance with the principles of **necessity, proportionality, transparency, accountability and respect for individuals' privacy and human rights**.

The Council recognises that surveillance may constitute the processing of personal data and will comply with applicable data protection legislation and guidance, including:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018;
- the Data (Use and Access) Act 2025;
- the Protection of Freedoms Act 2012;
- the Human Rights Act 1998;
- the Surveillance Camera Code of Practice;
- relevant guidance issued by the Information Commissioner's Office (ICO); and
- other relevant legislation, statutory guidance and codes of practice.

The Council will have regard to the Surveillance Camera Code of Practice when operating surveillance systems to which the Code applies.

The Council will not use surveillance simply because technology is available. Each surveillance system must have a clearly defined purpose, be necessary and proportionate for that purpose, and be subject to appropriate governance and review.

The Council cannot guarantee that all incidents within the coverage of a surveillance system will be observed or recorded.

## **2. Scope of the Policy**

This policy applies to:

- fixed CCTV systems;
- body-worn video cameras;
- dashboard and other vehicle-borne video cameras; and
- any future surveillance technology introduced by the Council which falls within the scope of data protection or surveillance-camera legislation.

The policy applies to Council employees, contractors and other persons authorised to operate, view, download, disclose or otherwise handle surveillance footage on behalf of the Council.

## **3. Purposes of Surveillance**

### **3.1 CCTV**

Torpoint Town Council's CCTV systems may be used to:

- assist in preventing, discouraging and investigating crime, vandalism and disorder;
- help reduce anti-social behaviour;
- protect Council property, buildings, facilities and equipment;
- promote the safety of employees, visitors and members of the public;
- assist in investigating health and safety incidents;

- assist the Police, Cornwall Council and other relevant enforcement or emergency services where lawful and appropriate;
- provide evidence for legal, insurance or enforcement purposes; and
- support the proper discharge of the Council's functions.

CCTV will not be used for routine monitoring of employees' performance.

### 3.2 Body-Worn Video

Body-worn cameras may be used by designated Council employees to:

- provide an accurate record of incidents;
- protect staff who may be placed in vulnerable or potentially confrontational situations;
- discourage threatening, abusive or inappropriate behaviour;
- support inspections and enforcement activities;
- support lone-working arrangements where there may be an increased level of risk;
- provide evidence where an incident occurs; and
- promote transparency and accountability when carrying out authorised Council duties.

### 3.3 Vehicle-Borne/Dashboard Camera

The Council's vehicle-borne camera may be used to:

- protect Council employees and Council vehicles;
- provide an evidential record of road traffic incidents and accidents;
- assist in investigating incidents occurring during the operation of the vehicle;
- assist with insurance claims;
- assist in the investigation of alleged criminal or anti-social behaviour where relevant; and
- support the safety and security of Council operations.

The dashboard camera will not be used for general monitoring of employees or members of the public.

## 4. Lawful Basis and Data Protection

Torpoint Town Council is the Data Controller for personal data processed through surveillance systems which it determines the purposes and means of processing.

The Council will identify and document an appropriate lawful basis under Article 6 of the UK GDPR for each surveillance activity and purpose.

Where the Council is carrying out its functions as a public authority, processing will generally rely upon **Article 6(1)(e) – performance of a task carried out in the public interest or in the exercise of official authority**, where the relevant legal and statutory framework supports that basis.

Where another lawful basis is appropriate and legally available, this will be identified and documented.

Where surveillance processing involves special category personal data or criminal offence data, the Council will identify and document any additional condition required under the UK GDPR and Data Protection Act 2018 before such processing is undertaken.

The Council will maintain appropriate records to demonstrate compliance with its data protection obligations.

The Council will ensure that surveillance processing complies with the data protection principles, including:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy, where applicable;
- storage limitation;
- integrity and confidentiality; and
- accountability.

## **5. Privacy and Proportionality**

Surveillance will only be undertaken where it is necessary and proportionate to achieve a clearly defined purpose.

The Council will apply privacy-by-design principles when installing, configuring or reviewing surveillance systems.

Where technically possible and appropriate, the Council will:

- position cameras to minimise unnecessary capture of private areas or neighbouring properties;
- use privacy masking where available;
- restrict camera fields of view;
- disable functions which are not required for the stated purpose;
- avoid unnecessary recording of areas where individuals have a heightened expectation of privacy; and
- regularly review whether camera positioning remains necessary and proportionate.

The Council will not intentionally monitor areas such as toilets, changing areas or other locations where there is a heightened expectation of privacy, except where a specific lawful and exceptional justification exists.

Covert surveillance will not be undertaken as part of normal Council operations. Any proposed covert surveillance must be separately assessed, authorised and undertaken only where lawful.

## **6. Data Protection Impact Assessments**

The Council will undertake and document a Data Protection Impact Assessment (DPIA):

- before introducing a new surveillance system where required by data protection legislation;
- before materially changing an existing surveillance system;
- where surveillance is likely to result in a high risk to individuals' rights and freedoms;
- where new surveillance technologies or functions are introduced; and
- where the nature, scale, location or purpose of surveillance changes significantly.

DPIAs will be reviewed where there is a significant change to the technology, purpose, coverage or method of operation.

The Council will maintain a register of surveillance DPIAs.

The DPIA for vehicle-borne surveillance will specifically consider the privacy rights of drivers, passengers and other individuals whose personal data may be captured. The DPIA for BWV will specifically consider the impact on individuals whose personal data may be recorded.

## **7. Signage and Transparency**

Surveillance operated by the Council will be overt.

Clear and appropriately positioned signage will be displayed to inform individuals that surveillance is taking place.

Where practicable, signage will identify:

- that surveillance is in operation;
- the organisation operating the system;
- the purpose of the surveillance; and
- how further information can be obtained.

CCTV signage will be positioned so that individuals have a reasonable opportunity to become aware of surveillance before or as they enter the relevant area.

Body-worn camera users will, where practicable, inform individuals that recording is taking place. Cameras will normally display a visible recording indicator when recording.

Appropriate signage will also be displayed within Council vehicles to inform drivers and passengers that vehicle-borne video surveillance is in operation.

The Council's Privacy Notice will provide further information about the processing of surveillance data.

## **8. CCTV Operation**

CCTV operated by the Council will be configured to collect only information necessary for its stated purpose.

The Council's fixed CCTV systems do not intentionally record audio and do not operate automatic number plate recognition (ANPR).

CCTV will normally operate continuously where continuous operation is necessary for the identified purpose.

CCTV will not be used for routine employee performance monitoring.

CCTV footage will only be reviewed where there is a legitimate operational reason, such as:

- a reported incident;
- a suspected offence;
- damage to Council property;
- an insurance claim;
- a health and safety incident;
- a safeguarding concern;

- a lawful request from an enforcement or emergency service; or
- another purpose identified within this policy.

## **9. Body-Worn Video Operation**

Body-worn cameras are surveillance systems and their use by the Council is subject to the UK GDPR, Data Protection Act 2018 and, where applicable, the Surveillance Camera Code of Practice.

BWV will be operated overtly.

BWV will normally remain switched off unless there is a reasonable expectation that recording is necessary and proportionate for an authorised operational purpose.

Where practicable, the officer should activate the camera before or at the earliest practicable point during an incident where recording is justified.

The officer should deactivate the camera when the purpose for recording has ended.

Where practicable, individuals will be informed that recording is taking place.

BWV should not be activated:

- for personal purposes;
- to record matters unrelated to Council duties;
- for routine monitoring of colleagues;
- in locations where there is a heightened expectation of privacy, unless there is a specific lawful and justified reason; or
- for any purpose outside the purposes authorised by this policy.

Where a member of staff considers that recording is necessary for safety or evidential purposes but cannot reasonably provide prior notification, recording may commence without prior verbal notification. The reason should be recorded where reasonably practicable.

Audio recording should be disabled unless the Council has specifically assessed, justified and authorised audio recording as necessary and proportionate.

BWV users will receive appropriate training before being authorised to operate a camera.

## **10. Council Vehicle Dashboard Camera**

The Council operates a dashboard/vehicle-borne camera in designated Council vehicles.

The dashboard camera is an overt surveillance system and will be used only for the purposes identified in this policy.

The camera is intended to record the area in front of the vehicle and will not intentionally record the interior of the vehicle unless specifically authorised following appropriate assessment.

The system will not intentionally record audio unless this has been separately assessed and authorised.

Where the system has functions such as GPS tracking, speed recording or other telematics, those functions will be assessed separately and will only be used where necessary and proportionate for an identified purpose.

The dashboard camera will not be used for general employee performance monitoring.

Appropriate signage will be displayed within the vehicle to inform drivers and passengers that video surveillance is in operation.

Access to dashboard-camera footage will be restricted to authorised Council officers and will only be permitted where there is a legitimate operational reason.

Footage may be viewed or downloaded where necessary for:

- a road traffic incident;
- an accident;
- an alleged offence;
- a health and safety incident;
- an insurance claim;
- damage to the Council vehicle or property;
- a complaint or investigation; or
- another legitimate purpose identified in this policy.

Where an incident has occurred, relevant footage may be preserved for longer than the routine retention period where necessary for an investigation, insurance claim, enforcement action or legal proceedings.

A DPIA will be undertaken for the dashboard-camera system where required by data protection legislation and will be reviewed following significant changes to the system or its operation.

## **11. Harvey Street Flats**

CCTV is installed at Harvey Street Flats, a property managed by Cornwall Housing Ltd (CHL).

Torpoint Town Council currently retains ownership of the CCTV equipment and acts as the Data Controller in accordance with the arrangements agreed with CHL.

The Council will provide a copy of this Policy to CHL.

## **12. Data Security and Access**

Stored surveillance footage will be securely protected against unauthorised access, alteration, disclosure, loss or destruction.

Access will be restricted to authorised personnel who have a legitimate operational requirement to access the footage.

The Council will maintain appropriate access controls and, where technically possible, audit logs showing access to recorded footage.

Employees with access to surveillance systems will receive appropriate training in:

- data protection;
- confidentiality;
- surveillance procedures;

- secure handling of footage;
- evidence management; and
- the requirements of this policy.

Surveillance footage must not be copied, downloaded, photographed, filmed or transferred except for an authorised purpose.

Footage must not be stored on personal devices, personal cloud storage, removable media or personal email accounts.

### **13. Retention and Deletion**

Routine CCTV recordings will be retained for a maximum of **31 days**, unless a shorter period is appropriate for a particular system.

The Council considers that this period provides a reasonable balance between the need to identify incidents which may not be reported immediately and the requirement to minimise the retention of personal data.

The Council will review this retention period periodically to ensure that it remains necessary and proportionate.

Footage will be automatically or manually deleted when the retention period expires, subject to technical limitations and the requirements of any applicable system.

Where footage is required for:

- an investigation;
- enforcement action;
- an insurance claim;
- legal proceedings;
- a complaint;
- a police investigation; or
- another legitimate and documented purpose,

the relevant footage may be retained for longer than 31 days.

Where footage is retained beyond the normal retention period, the reason for doing so should be recorded and the footage should be deleted when it is no longer required.

Different retention periods may be established for BWV or vehicle-borne video where justified by their particular purposes and documented within the relevant operational procedure.

### **14. Access to and Disclosure of Images**

Strict controls apply to the viewing and disclosure of surveillance footage.

Footage will only be accessed where there is a legitimate operational reason.

Only authorised Council employees may access recorded footage.

Footage may be disclosed to:

- the Police;

- emergency services;
- Cornwall Housing Ltd;
- relevant enforcement authorities;
- insurers;
- legal representatives;
- courts or tribunals; or

where there is a lawful basis and the disclosure is necessary and proportionate.

All disclosures will be recorded in an appropriate audit trail.

The Council will consider whether information can be shared lawfully before making any disclosure.

Where footage is provided to the Police or another enforcement body, the Council should retain an appropriate record of the request, recipient, date, purpose and footage supplied.

Where information is regularly shared with a third party, the Council will consider whether a formal data-sharing agreement is required.

## **15. Disclosure to the Media**

The Council will not disclose identifiable surveillance footage to the media unless there is a lawful basis for disclosure and the disclosure is necessary and proportionate.

Any proposed disclosure will be assessed in accordance with:

- data protection legislation;
- applicable exemptions;
- the Council's information-sharing procedures;
- any relevant legal or law-enforcement requirements; and
- the rights and freedoms of individuals appearing in the footage.

Where appropriate, footage may be anonymised, blurred or edited before disclosure.

The fact that footage may be considered to be in the public interest does not, by itself, provide a lawful basis for disclosure.

## **16. Data Subject Requests**

Where footage identifies an individual, it constitutes personal data.

Individuals have rights under data protection legislation, including the right to request access to their personal data, subject to applicable exemptions and restrictions.

Requests may be made verbally or in writing.

To assist the Council in locating relevant footage, applicants should provide, where possible:

- the date and approximate time;
- the location;
- a description of the incident;
- a description of themselves and, where relevant, their clothing; and
- any other information which may assist in locating the footage.

The Council may request reasonable and proportionate information to verify the applicant's identity where necessary to prevent disclosure of personal data to an unauthorised person.

The Council will normally respond to a valid Subject Access Request **within one calendar month** of receipt of the request and any information reasonably required to verify identity or clarify the request.

Where permitted by data protection legislation, the response period may be extended for complex or numerous requests.

The Council may withhold or redact footage where disclosure would adversely affect the rights and freedoms of other individuals or where another lawful exemption applies.

Where a request is refused in whole or in part, the Council will provide an explanation where legally required and will record the decision.

The Council will ensure that surveillance systems are capable, where reasonably practicable, of locating and retrieving footage relevant to a valid Subject Access Request.

## **17. Data Breaches**

Any loss, unauthorised access, disclosure, copying, alteration or other suspected compromise of surveillance footage must be reported immediately to the Town Clerk.

The Council will assess suspected breaches in accordance with its Data Breach Procedure and applicable data protection legislation.

Where required, the Council will notify the ICO and/or affected individuals within the applicable statutory timescales.

## **18. Complaints**

Individuals who have concerns about the operation of Council surveillance systems may complain through the Council's complaints procedure.

Individuals may also contact the Information Commissioner's Office where they consider that their personal data has not been handled appropriately.

The Council will maintain appropriate records of complaints concerning surveillance systems and will consider complaints as part of its annual surveillance review.

## **19. Governance and Responsibilities**

### **Town Clerk**

The Town Clerk has overall responsibility for the governance and compliance of the Council's surveillance systems.

Responsibilities include:

- ensuring that this policy is maintained;
- ensuring appropriate DPIAs are completed;
- ensuring appropriate lawful bases are identified;
- maintaining appropriate surveillance records;
- approving access arrangements;
- overseeing data-sharing agreements;
- ensuring appropriate training;
- reviewing complaints and incidents;
- liaising with the ICO and other relevant bodies where necessary; and
- ensuring that surveillance systems are reviewed regularly.

The Town Clerk will act as the Council's principal point of contact for surveillance-camera governance.

### **Operations Manager**

The Operations Manager is responsible for the operational management of surveillance systems used by the Operations Team, including authorised use of BWV and relevant vehicle-borne cameras.

Responsibilities include:

- ensuring authorised staff understand the operational procedures;
- ensuring BWV is used appropriately;
- ensuring relevant footage is preserved when required;
- reporting incidents or data breaches;
- maintaining appropriate operational records; and
- ensuring that surveillance equipment is used only for authorised purposes.

### **Community Hub and Library Manager**

The Community Hub and Library Manager may access CCTV footage where authorised and where there is a legitimate operational reason.

Any access, downloading or disclosure must comply with this policy and the Council's data protection procedures.

### **Cornwall Housing Ltd**

Authorised representatives can access footage at Harvey Street flats **only** and adhere to this Policy guidance.

### **Authorised Employees**

Employees authorised to operate or access surveillance systems must:

- comply with this policy;
- use surveillance equipment only for authorised purposes;
- maintain confidentiality;
- complete required training;
- protect surveillance footage from unauthorised access; and
- immediately report any suspected misuse, loss or breach.

## **20. Training**

Employees authorised to access or operate surveillance systems will receive appropriate training.

Training will cover, as relevant:

- UK GDPR and the Data Protection Act 2018;
- surveillance legislation and guidance;
- privacy and proportionality;
- operation of equipment;
- BWV activation and deactivation;
- dashboard-camera operation;
- handling and disclosure of footage;
- Subject Access Requests;
- evidence preservation;
- data breaches; and
- the Council's surveillance procedures.

Training will be refreshed where necessary and following significant changes to legislation, equipment or Council procedures.

Staff operating BWV will receive specific training on when to record, when recording should cease, providing privacy information, secure handling of recordings and responding to queries from members of the public.

## **21. Surveillance System Register**

The Council will maintain a register of surveillance systems.

The register should include, where applicable:

- system name and location;
- type of surveillance;
- purpose;
- areas covered;
- whether recording is continuous or event-triggered;
- audio capability;
- retention period;
- responsible officer;
- authorised users;
- relevant DPIA;
- signage arrangements;
- data-sharing arrangements;
- technical/security arrangements; and
- date of last review.

The Council will ensure that an operational requirement is documented for each surveillance system, setting out the identified need, purpose, required capabilities, coverage, operational arrangements and review arrangements.

The register will be reviewed at least annually.

## **22. Annual Surveillance Review**

The Council will undertake an annual review of each surveillance system to assess whether it remains necessary, proportionate and effective for its stated purpose.

The review will consider:

- whether the original purpose remains valid;
- whether the surveillance remains necessary;
- whether camera positioning remains appropriate;
- whether unnecessary areas are being captured;
- the number and nature of incidents recorded;
- complaints received;
- Subject Access Requests;
- disclosures to third parties;
- retention periods;
- security arrangements;
- equipment capability;
- staff training;
- privacy impacts; and
- whether the system should be continued, modified or discontinued.

The review will also consider relevant changes in legislation, ICO guidance and the Surveillance Camera Code of Practice.

The Council will use the current Surveillance Camera Code of Practice self-assessment tool, where applicable, to support its annual review and evidence compliance with the Code's principles.

## **23. Policy Review**

This policy will be reviewed at least annually, or sooner where required because of:

- changes in legislation;
- changes in ICO guidance;
- changes to the Surveillance Camera Code of Practice;
- introduction of new surveillance technology;
- significant changes to existing systems;
- a serious data breach;
- significant complaints;
- changes in operational requirements; or
- findings arising from a DPIA or annual surveillance review.

The Council will ensure that the policy remains consistent with the UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025 and other applicable legislation and guidance.

## **24. Council Contact**

### **Data Controller: -**

Torpoint Town Council  
1-3 Buller Road  
Torpoint  
Cornwall  
PL11 2LD

**Telephone:** 01752 814165

**Email:** [admin@torpointtowncouncil.gov.uk](mailto:admin@torpointtowncouncil.gov.uk)

The Council's Privacy Notice provides additional information about how personal data is processed and how individuals may exercise their rights.

## **25. Sources and Guidance**

This policy has been prepared with reference to the following legislation, statutory codes and official guidance. The Council should check the current versions of these sources when undertaking its annual policy review.

### **Legislation**

#### ***UK General Data Protection Regulation (UK GDPR)***

*The principal framework governing the processing of personal data, including the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, storage limitation, security and accountability.*

#### ***Data Protection Act 2018***

*Provides the UK statutory framework for data protection and supplements the UK GDPR, including provisions concerning criminal offence data and exemptions.*

#### ***Data (Use and Access) Act 2025***

*Amends aspects of the UK's data protection and privacy framework and should be considered when reviewing the Council's data-protection and surveillance arrangements.*

#### ***Protection of Freedoms Act 2012***

*Provides the statutory basis for the Surveillance Camera Code of Practice and establishes requirements relating to the use of surveillance camera systems in England and Wales.*

#### ***Human Rights Act 1998***

*Provides protection for Convention rights, including Article 8, the right to respect for private and family life, home and correspondence.*

#### ***Surveillance Camera Code of Practice – Guidance for Local Authorities, GOV.UK***

*The current government guidance confirms that local authorities, including parish and town councils, must have regard to the Surveillance Camera Code of Practice when operating surveillance camera systems to which the Code applies.*

*The guidance specifically identifies CCTV, body-worn video and vehicle-borne video systems as surveillance systems covered by the Code. It also sets out the Code's 12 guiding principles and recommends an operational requirement for each surveillance system.*

#### ***Surveillance Camera Code of Practice – Self-Assessment Tool***

*The Council may use the official self-assessment tool to assess and document compliance with the Code for individual surveillance systems. The tool specifically covers CCTV, BWV and vehicle-borne video systems.*

## **Information Commissioner's Office**

### **ICO – Video Surveillance, including Guidance for Organisations Using CCTV**

*The ICO's video-surveillance guidance addresses the data-protection requirements applying to CCTV and other surveillance technologies and includes guidance on accountability, the data-protection principles, governance, disclosure, individual rights and retention.*

### **ICO – Body-Worn Video (BWV)**

*The ICO's BWV guidance covers DPIAs, privacy information, staff training, retention and disposal, secure storage, access to recordings, Subject Access Requests and onward disclosure.*

### **ICO – Surveillance in Vehicles**

*The ICO's guidance on surveillance in vehicles covers vehicle-borne cameras and recommends consideration of DPIAs, clear signage for drivers and passengers, appropriate governance and retention arrangements, and limiting audio recording to exceptional circumstances.*

### **ICO – A Guide to Subject Access**

*The ICO's current Subject Access guidance explains the right of access under data protection legislation, including the applicable response requirements and changes arising from the Data (Use and Access) Act 2025.*