

Bishop's Stortford Town Council Body Worn Camera (BWC) Policy

1. Purpose and Scope

1.1 This policy sets out how Body Worn Cameras (BWCs) may be used by Bishop's Stortford Town Council ("the Council") staff when undertaking their duties in order to:

- Promote the safety of staff, councillors and the public.
- Prevent and deter aggressive, abusive or criminal behaviour.
- Capture best-available evidence of incidents, complaints or offences.
- Support the fair investigation of complaints and allegations against staff.

1.2 This policy applies to:

- Bishop's Stortford Market Staff.
- Events Staff.
- Other members of Town Council staff who are specifically authorised to use BWCs where necessary for their duties.

1.3 This policy does not apply to any covert recording. Covert surveillance is prohibited under this policy and may only be undertaken, if ever required, under separate statutory arrangements and authorisation.

2. Legal and Regulatory Framework

2.1 Use of BWCs must always be lawful, necessary and proportionate. In using BWCs, the Council and its staff must comply with, and have regard to, as applicable:

- Data Protection Act 2018 and UK GDPR.
- Human Rights Act 1998.
- Freedom of Information Act 2000.
- Protection of Freedoms Act 2012 and any relevant Surveillance Camera Code of Practice issued by the Home Office.
- Relevant guidance from the Information Commissioner's Office (ICO) on the use of surveillance and body worn video.

2.2 Nothing in this policy removes or reduces the requirement for staff to comply with criminal law, safeguarding legislation, health and safety duties, or internal Council policies including ICT, information governance, health and safety, lone working and safeguarding.

3. Roles and Responsibilities

3.1 Bishop's Stortford Town Council is the data controller for all personal data captured by Council BWCs.

3.2 Senior Responsible Officer (SRO)

The Events and Communications Manager is designated as the Senior Responsible Officer for BWC use, responsible for:

- Governance and oversight of BWC deployment.
- Ensuring appropriate training, procedures and monitoring are in place.
- Periodically reviewing the necessity and proportionality of BWC use.

3.3 System Administrator

The Market and Tourism Coordinator is the System Administrator responsible for:

- Day-to-day operation of the BWC system.
- Allocation and tracking of devices.
- Managing user access rights and passwords.
- Liaison with DCRS Ltd and any IT/hosting providers.
- Maintaining logs of access, export and disclosure of footage.

3.4 Authorised Users

Only Market Staff, Events Staff and other staff who have:

- Completed approved BWC training; and
- Been formally authorised by the SRO may use BWCs under this policy.

3.5 All authorised users are personally responsible for:

- Operating cameras in line with this policy and their training.
- Ensuring recordings are necessary, proportionate and time-limited.
- Reporting any malfunction, loss, misuse or data breach immediately through Council procedures.

4. When BWCs May and May Not Be Used

4.1 Justified Use

Authorised staff may activate BWCs where it is necessary and proportionate to:

4.1a) Record situations where they experience, or reasonably anticipate, verbal abuse, aggression, intimidation or threats.

4.1b) Record suspected criminal or anti-social behaviour encountered in the course of Council duties, including during markets, public events or work in Council-managed

spaces.

4.1c) Capture evidence of significant incidents, accidents or health and safety events where an objective record is required.

Routine, continuous recording of normal, non-confrontational interactions with the public is not permitted.

4.2 Prohibited or Restricted Use

BWCs must not be used:

4.2a) Covertly (i.e. hidden or deliberately concealed).

4.2b) For general surveillance of individuals or groups without a specific incident or lawful purpose.

4.2c) In situations where there is a heightened expectation of privacy (e.g. toilets, changing rooms, private dwellings), unless there is an immediate and serious risk to safety and no less intrusive option is available.

4.2d) For personal reasons, private disputes, or outside official Council duties.

4.2e) In any way that is discriminatory, harassing, or inconsistent with the Council's equality, dignity at work or safeguarding policies.

4.3 Special care must be taken when children, vulnerable adults or sensitive settings (such as schools, care homes or hospitals) are involved. In such cases, recording should only occur where necessary and proportionate, and for the minimum time required.

5. Operating Procedures

5.1 Allocation and Care of Equipment

5.1a) BWCs are Council property and will be issued to authorised Market Staff, Events Staff and other authorised staff as pool devices or individually assigned units as decided by the SRO.

5.1b) Before use, staff must check devices for damage, correct date/time and battery level and must report faults immediately.

5.1c) Cameras must be worn in a prominent position (typically on the chest) so they are clearly visible, and any recording indicator must not be obscured.

5.2 Notice and Activation

5.2a) As far as practicable and safe, staff must give a clear verbal warning before recording begins, stating that video and audio recording is about to commence and explaining the reason (for example: "I am now turning on my body worn camera to record this incident").

5.2b) If giving prior warning would escalate risk or is not possible, staff should provide the warning as soon as reasonably practicable once it is safe to do so.

5.2c) Recording should begin at the earliest opportunity when an incident or risk becomes apparent and should continue without unnecessary interruption until:

- The incident has concluded; or
- No further risk or legitimate purpose for recording exists.

5.3 De-activation

5.3a) Recording must stop as soon as it is no longer necessary and proportionate for the purpose for which it was started.

5.3b) Staff should, where safe, announce that recording has stopped.

5.3c) Devices should not be left running when travelling between incidents or during casual conversations with members of the public or colleagues.

5.4 Staff must not deliberately edit or partially record incidents in a way that could be misleading.

6. Data Management, Retention and Security

6.1 Uploading and Storage

6.1a) At the end of each shift, or as soon as practicable, staff must securely dock or upload BWC footage to the Council's approved storage system.

6.1b) The Council's approved storage is a web-based system via DCRS Ltd, and housed to a nominated PC, used in accordance with the Council's data protection and information security requirements.

6.1c) Footage must not be stored permanently on the device, on personal equipment, or transferred using unauthorised means (for example personal email, USB sticks or personal cloud accounts).

6.2 Metadata

Each recording should be associated with appropriate metadata such as date/time, location (if known), incident type, staff ID and any case or incident reference.

6.3 Retention

6.3a) The standard retention period for routine footage is 31 days, after which footage will be automatically deleted unless it has been flagged for longer retention.

6.3b) Footage may be retained for longer only where required for a specific purpose, such as:

- Ongoing criminal investigations or legal proceedings.
- Ongoing complaint or misconduct investigations.

- Formal health and safety or insurance investigations.
- Statutory record-keeping requirements.

6.3c) When the relevant purpose has concluded, retained footage must be securely deleted without undue delay in line with data protection principles.

6.4 Security and Access Control

6.4a) All stored BWC data must be protected by appropriate technical and organisational measures, including encryption at rest where supported, user authentication and access logging.

6.4b) Access to footage is strictly limited to:

- The SRO, System Administrator and other authorised managers who require access to perform their duties.
 - IT support personnel from DCRS Ltd or other providers working under contract, solely for system maintenance and subject to confidentiality and data protection obligations.
- c) Every access, copy or export of footage should be logged, including user, date/time, purpose and destination.

6.4c) Every access, copy or export of footage should be logged, including user, date/time, purpose and destination.

7. Use and Disclosure of Recordings

7.1 Internal Use

Recordings may be used for:

- a) Evidence in criminal investigations or prosecutions.
- b) Evidence in civil proceedings, insurance claims or formal investigations.
- c) Investigating complaints or allegations against staff, including disciplinary processes.
- d) Training, learning and service improvement, with anonymisation where possible.

7.2 External Disclosure

7.2a) Footage may be shared externally only where there is a lawful basis and it is necessary and proportionate, including with:

- Police and other law enforcement agencies.
- Legal representatives, courts or tribunals.
- Insurers or loss adjusters.

- Other public authorities where permitted or required by law.

7.2b) All disclosures must be authorised by the SRO or a delegated manager, documented in an access/disclosure log, and, where appropriate, subject to redaction (for example blurring of bystanders) to minimise unnecessary intrusion.

7.3 Recordings will not be released directly to the media or posted on social media by staff. Any media engagement involving footage must follow the Council's communications policy and legal advice.

8. Data Subject Rights and Requests

8.1 Individuals whose personal data is captured by BWCs have rights under data protection law, including the right to access their data (subject access request).

8.2 Requests for access, rectification, restriction or objection will be handled in line with the Council's Data Protection and Subject Access Request procedures.

8.3 Where providing a copy of footage would unjustifiably infringe the rights of others, the Council may redact or withhold parts of the footage as permitted by law.

8.4 Freedom of Information (FOI) requests for BWC footage will be dealt with under the Freedom of Information Act 2000. Personal data within the footage may be exempt from disclosure.

9. Training, Monitoring and Review

9.1 All authorised Market Staff, Events Staff and other authorised staff must receive training before first use and periodic refresher training. Training will cover:

- Legal framework and Council policy.
- When to commence and cease recording.
- Practical operation, safe use, and data security.
- Equality, diversity and human rights considerations.

9.2 The SRO will ensure periodic audits of compliance with this policy, including checks on device use, access logs, retention and deletion.

9.3 The effectiveness, necessity and proportionality of BWC deployment (including for market and events operations) will be reviewed at least every two years, or sooner in light of technological, legal or operational changes.

9.4 Any breach or suspected breach of this policy, including misuse of BWCs or unauthorised access or disclosure of footage, must be reported immediately through the Council's incident or data breach reporting procedures. Serious or deliberate

breaches may be treated as misconduct and may result in disciplinary action and/or regulatory or criminal investigation.