



Body-Worn Video (BWV) Policy

1. Purpose

London Warrant Enforcement Ltd (“LWE”) recognises the importance of Body-Worn Video (BWV) technology in supporting:

- The safety of staff, clients, and the public;
- Evidence capture for legal and regulatory compliance;
- Transparency and accountability in enforcement operations;
- Training, performance monitoring, and quality assurance.

This policy sets out the correct use, storage, and management of BWV devices in compliance with UK GDPR, the Data Protection Act 2018, and relevant enforcement regulations.

2. Scope

This policy applies to:

- All Enforcement Agents, field staff, and managers using BWV devices;
 - Administrative staff responsible for managing, storing, or reviewing BWV data;
 - All instances where BWV devices are deployed during enforcement visits, collections, or other operational activities.
-

3. Principles

LWE is committed to:

- Using BWV ethically, responsibly, and lawfully;
 - Recording all visit interactions, as required by the Enforcement Conduct Board, for transparency and compliance;
 - Protecting the privacy and rights of individuals captured on video;
 - Storing BWV recordings securely and limiting access to authorised personnel only;
 - Retaining BWV footage for a minimum of 3 months, in line with regulatory requirements;
 - Ensuring staff receive adequate training on BWV use, data protection, and consent.
-

4. Operation and Use

- BWV devices must be activated for all enforcement visits, including routine collections and case visits.
 - Recording should be continuous throughout interactions with debtors or members of the public.
 - Staff should inform individuals they are being recorded where practicable, unless doing so would compromise safety or operational integrity.
 - BWV devices must not be used for personal purposes or to monitor colleagues outside operational duties.
 - Devices must be maintained, fully charged, and operational at all times.
-

5. Data Protection and Privacy

BWV recordings are personal data under UK GDPR. LWE will:

- Collect and process footage lawfully, fairly, and transparently;
 - Limit access to authorised personnel only;
 - Store footage securely, with encryption and access controls;
 - Retain all visit recordings for a minimum of 3 months, unless required for investigation, legal proceedings, or longer retention obligations;
 - Avoid recording sensitive areas unless directly relevant to enforcement activity;
 - Handle subject access requests, disclosure, or deletion requests in line with UK data protection law.
-

6. Access, Disclosure, and Retention

- Only authorised managers or compliance staff may access BWV footage.
 - Footage may be shared with clients, courts, law enforcement, or regulators where legally required or permitted.
 - A log will be kept of all access, sharing, or deletion of BWV footage.
 - Footage will be securely deleted or anonymised after retention periods expire, unless required for ongoing investigations or legal purposes.
-

7. Training

All Enforcement Agents and relevant staff will receive training on:

- Proper use of BWV devices;
 - Legal and regulatory obligations regarding privacy and data protection;
 - Handling, uploading, and secure storage of recordings;
 - Reporting incidents or breaches related to BWV data.
-

8. Responsibilities

- Senior Management: Ensure compliance with legislation, regulatory guidance, and policy updates.
 - Managers and Supervisors: Monitor correct use, review footage as appropriate, and support staff training.
 - Enforcement Agents: Activate BWV for all visits, safeguard devices, and comply with privacy and operational requirements.
 - IT/Compliance Team: Ensure secure storage, access control, and retention scheduling.
-

9. Breaches and Disciplinary Action

Misuse, failure to record visits, or unauthorised access/disclosure of BWV footage is a serious breach and may result in:

- Disciplinary action, up to and including dismissal;
 - Notification to regulatory authorities or clients where required;
 - Referral to law enforcement where criminal offences are involved.
-

10. Policy Review

This policy will be reviewed annually, or sooner if:

- Legislation or industry guidance changes;
 - Operational or technological changes occur;
 - Breaches or incidents highlight the need for updates.
-