Audax®
BODY WORN VIDEO
MADE IN BRITAIN®

Body Worn Cameras

'10 things to consider in a BWV camera'

Video captured is fully admissible and increasingly used as vital evidence in court. Body worn video systems are critical technology for reducing threats and violence against police officers and other BWV users, improving policy and transparency in public relations, reducing offender complaints and speeding up the administration of justice.

1

Body Worn video needs to be Overt and obviously "a Camera" to meet legislation and guidance. BWV is to be used appropriately and proportionately to ensure safety, security and the privacy of people being recorded. (See guidance – Annex A)

People need to be made aware that they are being recorded both visibly (signage, lights Image etc) and audibly (tell them). Trials have shown that members of the public far less likely to behave in an abusive / aggressive manner if they know they are being recorded.

Covert recording of video and audio is generally illegal.

Audax BWV Camera hardware and software are designed from an early stage to guarantee security from camera to courtroom. A Security and Privacy by 'design' product.

Audax Global Solutions Ltd
+44 (0) 1752 264950 | info@audaxuk.com | www.audaxuk.com

2

Metadata

Records details of camera, date, user and location with each video. Metadata includes: Day / Hour / Minute / Second & GPS location all embedded (watermark) into Video. Device ID (5/6 digits) & Officer / User ID (5/6 Digits)
For evidential continuity, the correct time and date must always be visible in BWV footage. Proprietary software should not be required to view the time and date

For continuity, each recorded incident should have its own file or files, with a unique file name or code. The File name or code is not altered when the video file is transferred off the BWV camera.

3

User Access

It is important that the User has no access to erase, interfere or edit recordings and that the User has no access to the settings of the camera. Authentication such as a PIN password is required to replay any recording.

4

Memory and Encryption / Security

Cameras with removable memory (Micro SDHC cards etc) are not acceptable under DPA standards. Evidence can be deleted, cards can be removed and reformatted in any PC. Cards can be lost and thus a high potential of a Data Protection Breach.

Video recordings should be protected if the device is lost. Encryption is recommended by the Information Commissioners Office and Surveillance Camera Commissioner as an effective way to achieve data security. AES-128 and AES-256 are common standards for data encryption. Password Security and Encryption is only effective if access codes and authentication systems are correctly managed.

Video recordings should be erased from the device only after being transferred to and secured in the back-office system.

5

Battery

Removable batteries are not secure as the recording can be interrupted and thus the chain of evidence compromised etc. Battery Life – Should be capable of recording for a full shift.

6

Pre-Event and Post event recording.

To ensure no vital evidence is "missed" then the use of pre-event recording into a secure overwritten, non-accessible "buffer" is an accepted way of meeting privacy requirements as the recording isn't "live" until activated. There should also be Standard Operating Procedures to determine when the User activates and deactivates recording.

7

Environment and where it will be used.

Buy Cheap and buy twice – it isn't an excuse to inflate the price in the first place!

THE BWV needs to be Ruggedised and fit for continued use in demanding environments.

IP (Ingress Protection) rating is the UK standard measure of the device's resistance to dust and water. IP67 that is 'dust tight' and 'water proof up to 1m'

IK (Impact Protection) ratings are the UK standard measure that indicate impact protection from the device being dropped.

IP and IK ratings should be proven by certification by an independent testing laboratory otherwise there is no proof that the standards are met.

Every product imported into the UK needs to be CE marked and the certificate available for inspection.

If the products uses WiFi/3G/4G then EC-RED Certificate and EMC testing is a legal requirement.

Many "Grey" imports do not have these certifications. Why have products to reduce liability & aid in duty of care compliance that aren't compliant!

8

Video quality Minimum in 2021

720P HD thus producing an acceptable video recording under street lighting and inside buildings Minimum frame rate is 25fps (UK PAL standard)

Higher resolution and increased frame rates improve quality, but increase file size, data transfer time, and storage requirements.

Boosted low light level performance with the use of automatic / Selectable IR will improve useability of the BWV Camera but it does increase battery consumption.

9

Proprietary software

Often supplied on a disc with imported, low-cost BWV, is often unacceptable for use in the Criminal justice system. Proprietary file formats that require specialist replay software should not be used.

A Recording must be viewable in its original format using free software including VLC media player. When transferred or downloaded from the BWV camera, recordings should be preserved in their original format and any metadata retained.

In video terminology, a container file format (e.g. mp4, mov or avi) comprises a video codec (e.g. H264 or H265), an audio codec (e.g. mp3 or AAC) and information (e.g. technical metadata, time & date and subtitles)

10

Useful Additional Functions

- Ability to take a photograph while recording is activated is a better method of producing an image than acquiring a still from a video recording. High Quality JPEG image format is acceptable.

- Geo Tagging - Applies location data to image and video files.

- Generally limited to external locations

- Can improve the organising and retrieval of video within the back-office system.

- Wireless Connectivity – Wi-Fi 3G/4G/4G LTE

- Enables video with audio to be streamed from the BWV device to a control room and then displayed on a mobile display device such as a smartphone, tablet or laptop, as well as to a
- mobile command.

- BWV Recording and Video / Audio Live stream must be Encrypted. AES-128 and AES-256 are common standards for data encryption.

- Combined with GPS, allows a user's location to be monitored

- Recording can be activated and deactivated remotely.

- Note numerous inferior products utilise a mobile phone as a transitional step to 'live' stream video and audio onto the

- 3G/4G network but this brings all sorts of additional other issues into play such as phones having inferior batteries (additional device to issue, battery to charge etc) along with security of data, virus protection, unapproved APPs, questionable evidence chain with an additional device being used, user security etc.

About Audax®

Audax have been the worldwide **Pioneers in Body Worn Video (BWV) technology since 2005**. We are approved Members of **Made in Britain** as we design, develop and perform all final assembly, testing and quality control functions for our products at our Plymouth Headquarters. Silver members of **BAPCO** (for all professionals using or developing Public Safety technology); The **Guild of Security Industry Professionals** and accredited to the **Good Business Charter**; the Audax team is predominantly composed of service veterans and are proud to have the **Silver Award of the Armed Forces Covenant.**

Follow @audaxsolutions on Twitter
Follow @audaxglobalsolutionslimited on LinkedIn

Annex A:

The General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA)

The General Data Protection Regulations (GDPR) will be relevant to the retention of CCTV if the footage held is about a living person who can be identified from data. Articles 5 and 9 of the GDPR and Ss 34 to 42 of the DPA 2018 are the principles with which compliance is required.
https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

Protection of Freedoms 2012 (CCTV Codes of Practice: Aug 2013)

On the 12th August 2013, the Surveillance Camera Codes of Practice came into force. The Codes are pursuant to S30(1)(a) of the Protection of Freedoms Act 2012
https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Human Rights Legislation
https://echr.coe.int/Pages/home.aspx?p=home

In the picture: A data protection code of practice for surveillance cameras and personal information
Published by the The Information Commissioner's Office (ICO)
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
Of particular note Chapter 7.2 page 27

• BS 8593:2017 Code of Practice for Deployment and Use of Body Worn Video
• Body Worn Video Guidance – College of Policing 2014
• Technical Guidance for Body Worn Video Devices – UK Home Office – July 2018
https://www.gov.uk/government/publications/technical-guidance-for-body-worn-video-bwv-devices-cast-2018
• Safeguarding Body Worn Video Data – UK Home Office – 2018
https://www.gov.uk/government/publications/safeguarding-body-worn-video-bwv-data-2018

• Data Protection Guide for CCTV and Personal Information – ICO
• Data Protection Act 1998 via Information Commissioners Office

Surveillance Camera Commissioner

• https://www.gov.uk/government/organisations/surveillance-camera-commissioner

• Information Commissioners Office – Conducting Privacy Impact Assessments – Code of Practice – 2014

- https://ico.org.uk/for-organisations/guide-to-data-protection-1998/encryption/scenarios/body-worn-video/
- https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation