Code of Practice for operation and management of Body Worn Video Cameras

November 2024

Contents

1) **Introduction and Purpose**
2) **User Guidance**
3) **Data**
4) **Security and Governance**
5) **Relevant Legislation**
6) **MDDC Related Policies/Documents**

1. Introduction and Purpose

1.1. This Code of Practice will underpin oversight and day-to-day practice by all those managing and operating Body Worn Video (BWV). Everyone connected with BWV operated by Mid Devon and District Council (MDDC) will ensure that the principles and purposes outlined in this Code of Practice are always upheld. This Code of Practice should be read in conjunction with MDDC's CCTV and Surveillance Policy.

1.2. BWV involves the use of cameras that are worn by a person, and are often attached onto the front of clothing or a uniform. These devices are capable of recording both visual and audio information. It has been identified that the District Officers at MDDC within Environment and Enforcement are at a greater risk of confrontation due to the nature of their role. In order to ensure the health, safety, and wellbeing of the team, body worn video cameras are deployed on their persons.

1.3. The purpose of this document is to provide guidance on the use of BWV by officers within MDDC and ensuring compliance with relevant legislative requirements. For example: the deployment of BWV, retention of data and the security of data.

1.4. MDDC has opted to procure the D5 body camera (the device) provided by Reveal Media Ltd. This device is widely used by other authorities and Police forces throughout the country. The device is user operated and therefore, will only record when the user switches it on. This enables MDDC to ensure there is minimal intrusion on every day activities, its use is only ever activated when an officer believes themselves to be in a confrontational situation.

1.5. All users of the devices will be provided with the appropriate training for its use. This training will be conducted in-house utilising the knowledge and experience within MDDC. The Information Commissioner's Surveillance Code requires all staff to be trained in their responsibilities for data management.

2. User Guidance

2.1. The device is operated by the user and is not recording unless switched on using the switch located on the right hand side of the device. The device has a 30 second prerecord function, this will buffer 30 second recordings which enables the user to capture 30 seconds of footage prior to activation.

2.2. The user has to consider whether activation of the device is necessary, proportionate and addressing a need such as those listed in MDDC's CCTV and Surveillance Policy in section 3. Ultimately, it is for the user to determine when activation occurs based on the circumstance presented to them, however, consideration of these points should be used to justify the use. The user must ensure the device is functioning correctly and has the correct date and time prior to any duty commencing.

2.3. When activating the device users **MUST** inform those being captured that they are being recorded for visual and audio purposes. This ensures the user and MDDC are in compliance with the Data Protection Act 2018. This verbal announcement negates the need to have visible signage on the user's person. If it is not immediately possible to provide this announcement, recorded parties must be made aware at the earliest opportunity.

2.4. Once the device has been activated, users must ensure that recording is continuous throughout the interaction until it has reached a close. It is not acceptable for a user to switch the device on and off intermittently during an interaction.

2.5. Recording will always be of an overt nature and in a public place. No recordings are to be captured in what could be considered private dwellings, schools or care homes. The device has a front facing screen which any recorded party is able to see once the device is activated. Stealth/cloak mode is disabled on all devices.

2.6. Users should be acutely aware of their surroundings, careful consideration should be given to activating the device in areas surrounding schools or where vulnerable people may be present. Activation in circumstances such as this may require additional justification for use.

2.7. Where physical contact is made to a user, the device must be activated.

2.8. Playback directly from the device will not be available to the user. However, a passcode known to management and the Information Management team can provide playback from the device, should a Police Constable require it at the scene.

2.9. Direct recording of children and/or vulnerable people should be avoided. In extreme circumstance there may be a justifiable use of BWV in these circumstances, such as the user is being attacked by a person in either of these categories.

2.10. Device users are required to dock the devices upon their return to the office at the end of their shift.

2.11. The user is responsible for saving the captured footage directly to the encrypted cloud storage at the end of their shift.

2.12. Users will need to identify what footage is classed as evidential (and therefore retained) from a user footage sheet located within the office.

3. Data

3.1. Data captured from the device will be encrypted and only accessible via the use of DEMS 360 software. Within the authority there will be 1 devices which have the functionality to use DEMS 360. However, I.T are able to upload the software to further devices where required.

3.2. Any captured data will be deleted automatically unless marked evidential by the user.

3.3. Data marked as evidential will be retained for a period of 30 days. Once 30 days has elapsed the data will be automatically deleted from the system.

3.4. Where data has been identified for use in an ongoing Police investigation, this will be retained for a period of 2 years or until the case has reached a conclusion.

3.5. The device is self-contained and access cannot be obtained to the memory function. The device has built in memory storage and not a removable card to ensure security of data.

3.6. Storage of data will be via cloud provided by Reveal Media Ltd. This storage platform is an encrypted storage capacity which can only be accessed with the correct user credentials through DEMS 360 software.

3.7. In the unlikely event of a device becoming lost or stolen, users need to immediately report this in accordance with the Information Security Incident Policy to the . Access to any recorded data on the device is very unlikely, however, it is still considered a data breach and the relevant MDDC policies need to be followed in relation to this.

4. Security and Governance

4.1. Use of BWV described in this Code of Practice refers only to 'overt use' as there is no 'covert option.' MDDC should ensure that the use of the cameras is widely advertised prior to commencement, and that their use is reiterated by staff wearing a sign/symbol and/or making a verbal announcement where possible to those persons who may be recorded.

5. Relevant Legislation

5.1. This policy provides guidance on the appropriate and effective use of SCS and in particular how it meets the requirements of:

- The Human Rights Act 1998
- Data Protection Act 2018
- UK General Data Protection Regulation
- Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- Information Commissioners' CCTV Code of Practice

- Surveillance Commissioner's Surveillance Camera Code of Practice
- Criminal Procedure and Investigations Act 1996
- Criminal and Disorder Act 1998

6. MDDC Related Policies/Documents

- CCTV Code of Practice
- Data Protection Policy
- Freedom of Information Policy
- Information Security Incident Policy
- Records Management Policy