

BS 8593:2017



BSI Standards Publication

Code of practice for the deployment and use of Body Worn Video (BWV)

bsi.

AVA **Documents**
Document Sharing Hub

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2017

Published by BSI Standards Limited 2017

ISBN 978 0 580 95103 9

ICS 33.160.40

The following BSI references relate to the work on this document:

Committee reference GW/1/10

Draft for comment 17/30345717 DC

Amendments/corrigenda issued since publication

Date	Text affected

Contents

	Page
Foreword	ii
Introduction	1
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Planning and the operational requirements of BWV	3
4.1 General	3
4.2 Recommendations for the system owner	3
4.3 Deployment scenarios	5
<i>Table 1 — Example deployment scenarios</i>	5
5 Device recommendations	5
5.1 Essential functionality of BWV	6
5.2 Additional device considerations	9
5.3 Software and video management systems	9
6 Data management and security	12
6.1 General	12
6.2 General principles	12
6.3 Transfer of data for remote monitoring	14
6.4 Off-site storage	14
6.5 Sharing and redaction	14
7 Remote monitoring, escalation and response	15
8 Training and support	15
8.1 General	15
8.2 Supplier's own staff including temporary or subcontracted staff	15
8.3 User BWV training	15
8.4 Data handling training	16
8.5 Operator training	16
Annex A (informative) The eight principles of the Data Protection Act 1998	17
<i>Table A.1 — Eight principles of data protection</i>	17
Annex B (informative) Surveillance Camera Code of Practice — 12 guiding principles	17
<i>Table B.1 — 12 guiding principles of the Surveillance Camera Code of Practice</i>	17
Annex C (informative) Visible indication of the use of BWV — Graphic options	18
<i>Figure C.1 — Suggested graphics for users of BWV</i>	19
Bibliography	20

Summary of pages

This document comprises a front cover, and inside front cover, pages i to ii, pages 1 to 21, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 30 June 2017. It was prepared by Subcommittee GW/1/10, *Video surveillance systems (VSS)*, under the authority of Technical Committee GW/1, *Electronic security systems*. A list of organizations represented on this committee can be obtained on request to its secretary.

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

The word “should” is used to express recommendations of this standard. The word “may” is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word “can” is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this standard. Notes give references and additional information that are important but do not form part of the recommendations.

Commentaries give background information.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. “organization” rather than “organisation”).

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

Introduction

The proliferation and use of cameras to capture images and stream video footage continues to develop in both technical capability and in its attraction to the market. Every day, images are “captured” using a “camera” that can be shared on social media, make big news on television networks or be used as potential evidence to prove something has or hasn’t happened.

Technology has enabled CCTV to become a more personal feature of our everyday lives, most notably the use of mobile technology, such as phones and tablets, and more lately body worn video (BWV), which have cameras and audio as standard with the ability to upload video, images and audio (collectively referred to in this standard as “data”) either immediately or retrospectively to anywhere in the world. The consequences of this are widespread in terms of privacy and security.

The use of BWV clearly has its advantages in terms of providing the user with a sense of protection; a second pair of eyes and ears should something go wrong. It is, however, not without its challenges in terms of operational use, technical capability, security of data and privacy to those being recorded.

Legislation in the UK covers data protection and privacy, as well as the use of CCTV as evidence in both criminal and civil cases. Whilst technical standards and guidance exists, there are still many circumstances where extra guidance on the use, limitations and restrictions of CCTV is needed. The ICO has published a code of practice for CCTV (see *In the picture: a data protection code of practice for surveillance cameras and personal information* [1]) to promote good practice and attention is drawn to system owners' obligations under data protection law when processing personal data. This applies across all sectors in the UK.

With the complexities of CCTV, the government recognized the need to provide specific guidance for the use of surveillance cameras in public space and the Secretary of State issued the *Surveillance Camera Code of Practice* [2], which covers all forms of surveillance cameras including BWV.

This British Standard aims to support the work of the various public and private sector organizations to deliver a common framework on which BWV can be used appropriately and proportionately to ensure there is a balance between safety, security and the privacy of people being recorded. It provides recommendations that can be used consistently across multiple applications such as the police and criminal justice systems, parking and civil enforcement, lone workers and a common platform for integration into other technology and use.

1 Scope

This British Standard provides technical and operational recommendations for the deployment and use of Body Worn Video (BWV) used for the purposes of recording interactions between the wearer and other parties, or the environments in which the wearer finds themselves. This British Standard is applicable to both BWV users and system owners, as well as suppliers, taking into account how the visual/audio data is captured, viewed, stored and used securely.

NOTE Examples of where BWV might be used include emergency services, night-time economy (e.g. licenced premises), taxi marshalling, warden schemes, security guarding, parking enforcement and door supervision.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes provisions of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS EN 60529:1992+A2:2013, *Degrees of protection provided by enclosures (IP code)*

3 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1 alarm receiving centre (ARC)

continuously manned remote centre which receives activations from BWV and engages with users and response services

NOTE For further guidance on ARCs, see NPCC guidelines on police requirements and response to security systems [3], BS 8591, BS EN 50518 and BS 5979 (withdrawn).

3.2 body worn video (BWV)

device worn by a user that incorporates a camera, microphone and other software/hardware to enable the visual and audio recording, storage and subsequent exporting of its data for the specified deployment

NOTE Can also be referred to as "body worn camera (BWC)".

3.3 CCTV control centre

secure central location for a CCTV scheme, where images are collected, used, disclosed, retained or disposed of

[SOURCE: BS 7958:2015, 3.1]

3.4 control room

location where operational procedures are monitored and/or managed

[SOURCE: BS 7499:2013, 3.4, modified]

3.5 data

video and/or audio and associated metadata that comprises the recording from the BWV

3.6 data controller

person or organization that decides on the purposes for which and the manner in which any personal data are, or are to be, processed

3.7 operator

person specifically designated and authorized by the owner of an ARC, CCTV control centre or control room to monitor, respond and manage information received from a BWV

3.8 response services

response to an incident by the emergency services or other resources the system owner might have

NOTE Other resources could include a private security company or other service providers.

3.9 supplier

provider of a BWV system

3.10 system owner

individual or organization that contracts with a supplier to provide users under its employment or as part of a contract with BWV

NOTE The system owner is likely to be the data controller.

3.11 user

individual wearing and/or operating BWV

4 Planning and the operational requirements of BWV

4.1 General

System owners should take into account the operational requirements of any deployment of BWV and how any resultant data (video and audio) is to be managed, stored, redacted, shared and securely disposed. All stakeholders affected by a deployment should be given consideration; this includes the users (those asked to wear/use the BWV), those expected to handle or have access to data and those expected to react to an incident, if immediate action is required.

4.2 Recommendations for the system owner

4.2.1 Reason(s) to deploy BWV

The deployment of BWV should be based on legitimate reasons where personal data needs to be recorded. When deciding whether deployment is applicable or not, a privacy impact assessment (PIA) should be undertaken; possible examples of reasons are listed below.

- Employee safety/security – for example, if a risk assessment has been conducted and the user might encounter a specific risk from interfacing with people (physical attack or verbal abuse) or environmental factors (working in hazardous environments or where task-related risks might be present).
- Deterrent – for example, if the user is engaged in a job role where they might be policing or controlling a given environment/task which other people could choose to try and disrupt.
- Evidence capture – for example, if the user is involved in a role where they might witness or investigate criminal activity and capturing visual or audio evidence could help with the process of engagement with police or be used as evidence in legal proceedings (including possible civil action).
- Transparency – for example, where users regularly encounter complaints due to processes or interactions they undertake (policing, bailiffs, parking services).
- Environment monitoring – for example, using video to record changing environmental factors or share visual knowledge of an environment with others not present.
- Capturing data to use in process improvement or training – for example, identifying learning opportunities.

4.2.2 Activity to be observed

The principle activity or activities to be observed should drive the need for deployment, such as the following examples.

- Robbery/theft – for example, staff deployed in environments where the risk of robbery is present (retail, environments susceptible to metal theft, cash in transit).
- Verbal or physical abuse – for example, staff who have to deal with members of the public or recipients of services provided by the system owner and where discontent can occur.
- Incapacitation – for example, where staff are involved in job tasks which might be dangerous or carry hazard. In the event of incapacitation, video could be used to determine the nature of the incident and any environmental factors involved.

- Public safety – for example, where the user is operating in a wider environment where risk to the public might exist (crowd dynamic situations at large gatherings or security personnel operating at venues such as nightclubs, etc.).

4.2.3 Purpose of observation

The system owner should specify the precise nature and purpose of the observations to be made; examples could include the following.

- Identification – for example, of individual(s) involved in a crime.
- Monitor – for example, to provide situational awareness of the user's deployed environment to a control room or ARC.
- Verification – for example, using video from BWV to act as a supplementary source of intelligence/evidence.

4.2.4 Environmental factors

The system owner should take into account the environmental factors and risks that might be encountered by the user during their deployment; such as the following examples.

- Indoors/outdoors – different lighting, temperature, weather conditions might occur if the user is operating indoors, outdoors or a mix of both. Locating the user (for example, in the event of an incident) might also be challenging if they are indoors or outdoors.
- Location – does the job that the user undertakes occur in a single location (e.g. a retail store, door point) or is the user more mobile? Different locations might have different environmental factors.
- User activity – what activity is the user carrying out and where would the BWV be located on the user.
- Pre-identified risks – for example, is the wearer likely to be engaging with known aggressors or members of the public who might have conditions that affect their behaviour (e.g. mental health issues, alcohol or drug addiction issues). Pre-identified risks might also relate to the location/geography of the work conducted (e.g. urban, suburban, rural).

Once the system owner has taken into account the above factors, they should evaluate which of the deployment scenarios detailed in [4.3](#) are most applicable to their application need.

4.2.5 Privacy impact assessment (PIA)

A PIA should be undertaken at an early stage and be periodically reviewed to ensure that the purpose of the system is and remains justifiable. Where appropriate and possible, there should be consultation with those most likely to be affected, and the impact on their privacy should be assessed and any appropriate safeguards put in place.

NOTE 1 Comprehensive guidance on undertaking a PIA is available from the Information Commissioner's Office [\[4\]](#).

NOTE 2 Attention is drawn to the Data Protection Act 1998 [\[5\]](#) and the General Data Protection Regulation [\[6\]](#). The eight principles of the Data Protection Act 1998 are given in [Annex A](#).

4.2.6 Guiding principles and self-assessment tool (SAT)

COMMENTARY ON 4.2.6

The Surveillance Camera Code of Practice [\[2\]](#) gives 12 guiding principles for end users to take into account before acquiring and when using and when auditing a CCTV surveillance system. See [Annex B](#).

To help achieve compliance with the 12 guiding principles of the *Surveillance Camera Code of Practice* [\[2\]](#), a suitable self-assessment tool should be used to ensure the purpose of using BWV is appropriate

and proportionate to the need of the person wearing the device. The tool should also address the needs of those that are being recorded to ensure privacy is respected.

NOTE The Surveillance Camera Commissioner's website contains a self-assessment tool specifically for BWV, which provides a questions and answer tool to ensure the 12 guiding principles of the Surveillance Camera Code of Practice [2] are considered. See <www.gov.uk/government/publications/surveillance-camera-code-of-practice-self-assessment-tool> [last viewed 2 June 2017].

4.3 Deployment scenarios

COMMENTARY ON 4.3

Recording and the storage/use of data from BWV can occur in a number of different ways; the following describes the most common (see also Table 1).

The system owner should evaluate which scenario is best for their given application, as there are considerations for both the procuring party and the user.

- 1) Scenario 1 – BWV with local (on-device) storage of visual and/or audio data, with subsequent transfer of data to a local computer for review and storage.
- 2) Scenario 2 – BWV with local (on-device) storage of visual and/or audio data, with subsequent transfer of data via an internet connection to a remote storage location (e.g. data centre).
- 3) Scenario 3 – BWV with local (on-device) and transferred (off-device) storage of visual and/or audio data, with live (or near live) transfer of data via a wireless (e.g. Wi-Fi or cellular) internet connection to a CCTV control centre or control room.
- 4) Scenario 4 – BWV with local (on-device) and transferred (off-device) storage of visual and/or audio data, with live (or near live) transfer of data via a wireless (e.g. Wi-Fi or cellular) internet connection to a remote ARC for the purpose of monitoring and/or escalation to a responder (e.g. emergency services or third-party security).

Table 1 — Example deployment scenarios

Deployment scenario	Device storage	Data transfer connectivity	Data location
Scenario 1	Visual/audio	Local only	Local computer/storage device only
Scenario 2	Visual/audio	Local and remote	Local and remote storage, e.g. data centre, cloud storage
Scenario 3	Visual/audio	Local and remote including live/near live transfer	Local and remote management, review storage to a CCTV control centre or control room
Scenario 4	Visual/audio	Local and remote including live/near live transfer	Local and remote storage to an ARC

5 Device recommendations

COMMENTARY ON CLAUSE 5

This clause details recommended features for BWV and other associated software, network and storage considerations where appropriate. These recommendations relate to the security, data management, functionality and simplicity of BWV systems.