



DPC: 25 / 30486873 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 24 February 2025

Origin: National

Latest date for receipt of comments: 22 April 2025

Project No. 2024/00312

Responsible committee: GW/1/10 Video Surveillance Systems (VSS), commonly known as CCTV

Interested committees: IST/44, ART/1, IST/33

Title: BS 8593, The deployment and use of body worn video (BWV) - Code of practice

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 22 April 2025**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Editorial Project Manager: **Lorna Wroe**

Direct tel:

E-mail: lorna.wroe@bsigroup.com

Introduction

Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international and European standards, comments will be reviewed by the relevant UK national committee before submitting the consensus UK vote and comments. If the draft standard is approved, it is usual for the resulting published standard to be adopted as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

Annotated drafts are not acceptable and will be rejected.

All comments should be submitted online at <http://standardsdevelopment.bsigroup.com>. You will need to register in order to comment.

BS 8593:2025

The deployment and use of body worn video (BWV) – Code of practice

IMPORTANT INFORMATION

Please note that this is a draft and not a typeset document. Editorial comments are welcomed, but persons commenting on this draft are advised not to comment on detailed matters of typography and layout.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on XX/XX/XXX. 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 these committees can be obtained on request to the committee manager.

Supersession

This British Standard supersedes BS 8593:2017, which is withdrawn.

Information about this document

This is a full revision of the document, and introduces the following principal changes:

- content relating to the Data Protection Act 1998 [1] has been updated to relate to the Data Protection Act 2018 [2];
- the privacy impact assessment (PIA) that was part of the Data Protection Act 1998 [1] has been replaced by a data protection impact assessment (DPIA)-focused approach;
- the term “closed circuit television” (CCTV) has been replaced by “video surveillance systems” (VSS); and
- a new **6.5.3** has been introduced to provide recommendations on disclosing body worn video (BWV) data to the press or media.

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at knowledge.bsigroup.com, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Use of this document

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

Users may substitute any of the recommendations in this British Standard with practices of equivalent or better outcome. 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 document 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 document. 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 document. 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 has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient’s own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute 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 made Video Surveillance Systems (VSS) a more personal aspect of our daily lives, primarily through mobile devices such as mobile phones and tablets and increasingly through body-worn video (BWV) cameras. These devices come equipped with cameras, audio and recording, and radio transmission capabilities that allow for the immediate or retrospective uploading of video, images, and audio (collectively referred to in this standard as “data”) anywhere in the world. The consequences of this are widespread in terms of privacy and security.

The use of BWV offers clear advantages such as providing the user with a sense of protection; and having 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 addresses data protection and privacy, as well as the use of VSS as evidence in both criminal and civil cases. While technical standards and guidance exists,

there are still many circumstances where extra guidance on the use, limitations and restrictions of VSS is needed. The Information Commissioner's Office (ICO) has published a code of practice for VSS (see *In the picture: a data protection code of practice for surveillance cameras and personal information* [3]) 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.

Recognising the complexities of VSS, the government has provided specific guidance for the use of surveillance cameras in public space. The Secretary of State issued the *Surveillance Camera Code of Practice* [4], which covers all forms of surveillance cameras including BWV.

When processing data to be used as evidence, attention is drawn to the Forensic Science Regulator's code of practice [5], which states that all data handling, especially in forensic contexts, needs to meet established regulatory expectations.

This British Standard aims to support the work of the various public and private sector organizations by providing a common framework for the appropriate and proportional use of BWV, enabling 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 and lone workers, it also provides 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) for recording interactions between the wearer and other parties, or the environments in which the wearer finds themselves. This British Standard is applicable to BWV users, system owners and suppliers, taking into account how the data is captured, viewed, stored, handled and retained 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, or limits the application, of this document¹⁾. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 7499:2013, *Static site guarding and mobile patrol service – Code of practice*

BS 7958:2015, *Closed circuit television (CCTV) – Management and operation – Code of practice*

BS ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*

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

3 Terms and definitions

For the purposes of this document, 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

¹⁾ Documents that are referred to solely in an informative manner are listed in the Bibliography.

NOTE For further guidance on ARCs, see NPCC guidelines on police requirements and response to security systems [6], 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, other hardware and software to enable the visual and audio recording, live transmission, storage and subsequent exporting of its data for the specified deployment

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

3.3 control room

location where operational procedures are monitored and/or managed

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

3.4 data

video and/or audio and associated metadata (e.g. storage location, identifiers, geolocation, time, date, audit trail [e.g. buttons pressed]) that comprises the recording from the BWV

3.5 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

3.6 data destination

location that stores data from BWV (e.g. Video management System [VMS], Evidence Management System [EMS], Cloud data centre).

3.7 operator

person specifically designated and authorized by the owner of an ARC, VSS 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 controller

integration and system management point for BWV

NOTE Can also provide temporary storage of data for high-speed offloading of BWV data before transferring to the data destination.

3.11 system owner

legal person or entity, agency or individual designated as having overall responsibility for the formulation and implementation of the policies, objectives and control of a BWV system

NOTE 1 The owner also has responsibility for all statutory responsibilities, including the role of "data controller" (see the Data Protection Act [2])

NOTE 2 The owner could be a partnership, provided it has a formal constitution.

3.12 user

individual wearing and/or operating BWV

3.13 video management system (VMS)

software installed locally on computers, installed within an organisations' network, or accessed online, that primarily enables the management of video footage produced by BWVs, including but not limited to viewing, editing, sharing and deletion

NOTE 1 Other functions may include managing the status, configuration and firmware of BWVs, viewing live camera geolocations, and generating management information around the BWV usage and status.

NOTE 2 Some of these functionalities may reside in the system controller.

3.14 video surveillance system (VSS) control centre

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

[SOURCE: BS 7958:2015, **3.1**, modified]

4 Planning and the operational requirements of BWV

4.1 General

The system owner should take into account the operational requirements of any deployment of BWV and how any resultant data (video and audio) is to be securely managed, stored, redacted, shared and disposed of. The impact on all stakeholders affected by a deployment should be assessed; this includes the users (those asked to wear/use the BWV), those who might be recorded, those expected to manage, 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 need. When deciding whether deployment is applicable or not, a Data Protection Impact Assessment (DPIA) should be undertaken; possible examples of reasons are listed below.

- a) 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), it gives the ability for users to raise alarms to get help and assistance.
- b) 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.
- c) Evidence capture – for example, if the user is 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).
- d) Transparency and accountability – for example, where users regularly encounter complaints due to processes or interactions they undertake (policing, bailiffs, parking services).
- e) Environment monitoring – for example, using video to record changing environmental factors or share visual knowledge of an environment with others not present.
- f) Capturing data to use for training, organizational learning, and for individual professional development.
- g) Location tracking – for example, confirmation of a person's location (visually or using positioning information).

4.2.2 Activity to be observed

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

- a) Robbery/theft – for example, staff deployed in environments where the risk of robbery is present (retail, environments susceptible to metal theft, cash in transit).

- b) 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.
- c) 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.
- d) Public safety – for example, where the user is operating in a wider environment where risk to the public might exist (e.g. crowd dynamic situations at events, anti-social behaviour, etc.).
- e) Environmental monitoring and surveying – for example, monitoring of a process or task for maintenance and audit trail of processes.

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:

- a) Identification – for example, of individual(s) involved in a crime.
- b) Situational monitoring and management – for example, to provide situational awareness of the user's deployed location/environment to a control room or ARC, which may result in the escalation and coordination of responses.
- c) 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 assess the environmental factors and risks that might be encountered by the user during the deployment and storage of the equipment and data; such as the following examples.

- a) Indoors/outdoors – different lighting (artificial or natural), temperature, sterile environments, explosive atmospheres, or weather conditions might occur if the user is operating indoors, outdoors or a mix of both.
- b) Electromagnetic interference – would BWV equipment and other equipment interfere with each other (e.g. medically implanted devices, large generators, etc.)?
- c) 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 that affect performance around location accuracy.
- d) Activity – what activity needs to be observed and where would the BWV be located on the user (e.g. chest or head).
- e) 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).

This assessment should be used to evaluate which of the deployment scenarios detailed in **4.3** are most applicable to their application need.

4.2.5 Privacy and disclosure issues

4.2.5.1 General

A DPIA should be used to assess the potential impact of processing personal data on individuals' privacy rights. This should be conducted before starting any data processing

activity. The organization should identify and mitigate risks associated with data processing activities. The organization should:

- a) identify the processing activity: clearly define the purpose, scope, and context of the data processing;
- b) assess necessity and proportionality: evaluate whether the processing is necessary and proportionate to the intended purpose;
- c) identify risks: identify potential risks to individuals' rights and freedoms;
- d) implement mitigation measures: propose measures to minimize risks (e.g. pseudonymization, encryption, access controls);
- e) consult stakeholders: involve relevant parties (data subjects, data protection officers, etc.) in the assessment;
- f) document findings: maintain a record of the DPIA process and outcomes;
- g) define, and give examples of, when BWV should be activated and when it should not be activated; and
- h) engage with the ICO, prior to starting any data processing activity, if a high-risk data processing activity has been identified in the DPIA.

4.2.5.2 Data disclosure

4.2.5.2.1 BWV data handling and disclosure principles

The BWV data handling and disclosure principles are:

- a) recorded material should only be processed for specified, lawful purposes and purpose limitation requirements; and
- b) access to, handling, distribution, and deletion of recorded material should strictly follow established procedures, ensuring integrity and confidentiality.

NOTE Attention is drawn to the seven principles of Data Protection (see Annex A), as outlined in the Data Protection Act 2018 [2]

4.2.5.2.2 Third-party requests

Third parties (such as law enforcement agencies, statutory authorities, solicitors, and others) should request data from the VMS for various purposes, including:

- a) providing evidence in criminal or civil proceedings;
- b) contributing to crime prevention and reduction efforts;
- c) identifying witnesses; and
- d) serving the public interest.

System owners should not obstruct legitimate third-party investigations or destroy relevant data.

4.2.5.2.3 Subject access requests

When responding to subject access requests, system owners should:

- a) verify the validity of the request;
- b) provide specific data relevant to the request; and
- c) obscure any unnecessary personal data.

If on-site obscuring is not feasible, data can be sent to an editing house for processing.