

Appropriate Policy Document – Body Worn Video to General Public (Wholly Exceptional)

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

You should read this document alongside our [Privacy Notice](#).

Description of data processed

A brief description of each category of SC/CO data processed.

This process involves the viewing of potentially Un-redacted Body worn video footage from recorded encounters of interactions between police and members of the public. BWV devices are primarily designed to record encounters between police officers and members of the public. Not only do they record both video and audio, but they employ wide angle lenses that capture events across a broad field of view. This can result in the capture of larger amounts of information from a) the subject of the recording, b) other persons present at the time of the recording, c) unrelated 3rd parties inadvertently captured in audio or video during the recording.

Examples of the data captured are:

Personal Data

Name

Age/date of birth

Address

The data subjects' physical attributes through the moving images

Police Officers ID Number (Shoulder number)

All individuals Location Data

Special Category Data

Any of the special categories of data could be processed as part of the viewing, namely:

personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) data concerning health;



(d) concerning an individual's sex life or sexual orientation.

Additionally, criminal convictions data may be processed in the course of PNC checks being carried out, which are then disclosed to the CMG members.

- Once a Body worn video recording has been made the recorded data becomes police information, and is subject to the Code of Practice on the Management of Police Information (MoPI).
- The MPS's guidance requires that all BWV footage should be uploaded from the camera as soon as practicably possible. Once the footage is uploaded the video is deleted from the camera.
- Body worn video footage is uploaded and stored in the UK based Microsoft Azure Cloud. It is accessed via the MPS evidence management system evidence.com.
- Once footage has been uploaded the recording officer/ investigating officer then has to make a decision as to whether that footage will be required at a later date either as evidence/relevant material or for a policing purpose.
- If the footage is assessed as required, it is retained under MoPI provisions for evidence, disclosure or other policing purpose.
- If a retention category is not selected the footage will auto delete from the system after 31 days.
- Body Worn video footage viewed as part of this process remains within the evidence.com system, no copies are made and the footage is not altered or edited as part of the viewing process.
- Footage is not retained solely for the purpose of this viewing process.

Schedule 1 condition for processing

The name and paragraph number of our relevant Schedule 1 condition(s) for processing.

Pursuant to s.10(3) DPA, the processing matches the requirement by meeting the following condition in Part 2 Schedule 1 DPA:

Paragraph 6: Statutory etc and government purposes

(1) This condition is met if the processing—

(a) is necessary for a purpose listed in sub-paragraph (2), and

(b) is necessary for reasons of substantial public interest.

(2) Those purposes are—

(a) the exercise of a function conferred on a person by an enactment or rule of law;

(b) the exercise of a function of the Crown, a Minister of the Crown or a government department.

Procedures for ensuring compliance with the principles

There is also no requirement to reproduce information which is recorded elsewhere – **questions may be answered with a link or reference to other documentation, to your policies and procedures, Data Protection Impact Assessments (DPIAs) or to your privacy notices.**

Accountability principle

The legal framework and existing body of guidance in which the MPS relies is provided by the following:

- The Data Protection Act 2018 (including Compliance Policy and Guidance).
- NPCC Authorised Professional Practice (APP).
- NPCC (2005) Guidance on NIM, NIM Guidance and NIM Codes of Practice (2005).
- APP Intelligence Management Guidance.
- 2010 Guidance on the Management of Police Information.
- The APP Data Protection Manual of Guidance.
- MetSec Code.
- MPS Information Management Support Pages.
- MPS Records Management Policy (including the Retention, Review and Disposal Schedule).

Principle (a): lawfulness, fairness and transparency

In the exercise of its core functions, the MPS processes personal data for the “law enforcement purposes” as set out in Part 3 DPA, which incorporates the Law Enforcement Directive into domestic law. The law enforcement purposes are found in s.31 DPA.

The processing i.e. the sharing with the public of the BWV footage in **wholly exceptional circumstances** will be individual case specifically demonstrated as *necessary* for the law enforcement purposes. And further, to be lawful within the Part 3 DPA regime the processing (sharing of BWV) will have been evidenced by the NPCC Commander to be **strictly necessary** since much of the data processed during the MPS’ policing activities may be subject to the sensitive processing requirements as set out in s.35(3) DPA.

In order to carry out sensitive processing, where the MPS is not relying on the consent of the data subject, the MPS fulfils criteria from s.35(5) DPA.

In the exceptional circumstances that give rise to strict necessity, the MPS relies on the following Schedule 8 condition:

1 Statutory etc purposes

This condition is met if the processing—

(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and

(b) is necessary for reasons of substantial public interest.

In fulfilment of the above condition, the MPS relies upon on Schedule 4 Police Reform & Social Responsibility Act 2011 arguing that the processing is necessary to promote and regain public confidence, and that this is in the substantial public interest having regard to a specific and serious threat. In addition to the above, the data may fall within the definition of “criminal convictions” data as set out in s.11(2) DPA.

The processing of special category data is in accordance with Art 9(2)(g) GDPR.

Principle (b): purpose limitation

The intended processing is in line with the purposes outlined, those listed in the [Privacy Notice](#) and our notification with the Information Commissioner's Office: Registration No: Z4888193.

Principle (c): data minimisation

The MPS will not process exhaustive amounts of personal information on the loose premise that it may be useful now or in the future. The MPS is only interested in processing data that is relevant to our policing purpose.

If at any point, the data processed is found to be excessive to the purpose, then the processing may be ceased. The processing will be subject to periodic yearly review in terms of assessing the value that this product plays in enabling the MPS to meet its policing purposes.

Principle (d): accuracy

The MPS is mindful of the potential damage and distress to the data subject, the organisation and to third-parties if the data processed was inaccurate in anyway. To mitigate this, an ongoing examination of the accuracy and quality of the data will occur throughout the course of the processing.

Principle (e): storage limitation

The information will be retained in line with our [Records Management Policy](#) and [MoPI](#) obligations.

Principle (f): integrity and confidentiality (security)

Only authorised personnel have access to the MPS's systems; the data is encrypted in transit and while at rest in storage.

Retention and erasure policies

The footage is not retained solely for the purpose of this process and any footage that is not retained as evidential for a policing purpose auto-deletes from the evidence management system after 31 days

The information will be retained in line with our [Records Management Policy](#).

APD review date

One Year from date of publication.