



Home Office

Safeguarding Body Worn Video Data

Published October 2018

Publication No.011/18



Author: Toby Nortcliffe

Contributor: Dominic Martin (Section 4)

Safeguarding Body Worn Video Data

Version 2.0

Publication No 011/18

ISBN 978-1-78655-627-1

FIRST PUBLISHED 2018

© Crown copyright 2018

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Home Office
2 Marsham St
London
SW1P 4DF
United Kingdom

www.homeoffice.gov.uk/



Foreword

“Police forces across England and Wales have seen a dramatic increase in the use of Body Worn Video (BWV) cameras over recent years. Estimates for the end of 2018 suggest that there will be about 80,000 BWV cameras in operational use. However, with the increased use of BWV comes a greater risk of loss of personal or sensitive data.

Front-line policing is inherently confrontational and frequently highly unpredictable, therefore it is an unavoidable fact that there will be losses of cameras, resulting in the potential loss of personal and sensitive data. Fines imposed by the Information Commissioner’s Office (ICO) can be significant if data controllers have failed to mitigate against these risks. It is therefore imperative that police forces understand the risks of not providing adequate measures to mitigate against these potential risks.

As the national lead for body worn video I have been working with the Home Office, the Information Commissioner and the Surveillance Camera Commissioner to produce this document on safeguarding data for BWV cameras. The purpose of this document is to prevent data loss in order to protect the public while ensuring operational effectiveness of this relatively new technology. This revised version takes into account recent changes to Data Protection legislation and includes new guidance on redacting BWV recordings for Subject Access Requests. Accompanying this document will also be a revision of the [Technical Guidance for Body Worn Video Devices](#). This revision will help ensure that the BWV devices currently being purchased and deployed meet an appropriate minimum technical standard in order to achieve the best evidence possible.”

A handwritten signature in black ink, appearing to read 'Andy Marsh', is written over a light blue horizontal line.

Chief Constable Andy Marsh, NPCC Lead for Body Worn Video

Introduction

The aim of this document is to provide a practical understanding on the wide range of information that Body Worn Video (BWV) devices are able to capture and what safeguards can be implemented to avoid losing this data. This revised version takes into account the Data Protection Act 2018 (DPA18) and the General Data Protection Regulation (GDPR).

Safeguarding BWV data requires far broader consideration than just encryption and thought should be given as to where the weakest security points are within the whole process. This starts with the BWV device itself and continues with the transfer of data and its storage as well as sharing with the Criminal Justice System (CJS) and in some cases the public. However it is crucial to consider the human element within this process especially with regard to training not only for users of these devices, but also for anyone involved with the handling or management of BWV data.

Overall a balance is required between implementing measures to safeguard BWV data and ensuring that the operational effectiveness of BWV is not compromised.

The document contains the following sections:

1. Data recorded by BWV devices
2. Consequences of losing BWV data
3. Measures to safeguard BWV data
 - 3.1 Physical security of BWV devices
 - 3.2 Protecting data on BWV devices
 - 3.3 Transferring data to back office system
 - 3.4 Tagging and organising data
 - 3.5 Asset management of BWV devices
4. Distributing BWV data
 - 4.1 Sharing data for policing purposes
 - 4.2 Releasing data for Subject Access Requests
 - 4.2.1 Visual data redaction
 - 4.2.2 Audio data redaction
 - 4.2.3 Output data

Other publications that complement this guidance are:







[Technical Guidance for Body Worn Video Devices](#) - Home Office, July 2018

[Encryption guidance](#) - Information Commissioner’s Office, March 2016

[CCTV Code of Practice](#) - Information Commissioner’s Office, May 2015

[Guide to Law Enforcement Processing \(Part 3 of the DP Act 2018\)](#) - Information Commissioner’s Office, 2018

[Surveillance camera code of practice](#) - Surveillance Camera Commissioner, June 2013

KEY			
	Audio		Good practice
	Visual		Advice
	Metadata		Training points

Colour has been used in this publication to convey information; should it be printed in black and white some of this will be lost.

1. Data recorded by BWV devices

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 much larger amounts of information than the User intended and this is especially true of devices with High Definition (HD) cameras that record information in greater detail than those using Standard Definition (SD).











A short recording from a BWV device can provide compelling evidence for a criminal investigation. However, that recording is also likely to contain information that while not crucial to an investigation could still be considered sensitive in nature. If any of the recorded information is accessed by an unauthorised third party then this could not only compromise a police investigation, but also risks causing considerable intrusion into a person's privacy at a time of vulnerability. One example is the risk of unintentionally identifying a person and the considerable harm that could result.

Small traces of sensitive information may have little significance when considered independently. However, when linked over an entire recording timeline the significance can be considerable. Furthermore when traces are linked across several recordings especially from a number of devices with different view points, and with other non-BWV data, then this significance could escalate.

The following tables and images demonstrate the wide range of information that can be captured by BWV devices. This can be classed as primary information that is intentionally recorded to benefit a police investigation and secondary that is unintentionally recorded and while not relevant to a police investigation, could be considered sensitive. Furthermore there are special locations such as a hospital, place of worship or private home where the potential for recording sensitive information is much greater.























Primary Information

Examples of data the User **intends** to capture that can benefit a police investigation and act as evidence.

	First accounts from victims, suspects or witnesses
	Identification of a person
	Direct conversations with members of the public
	Decisions and actions of the BWV User
	Physical and mental state of people
	Demeanour of people
	Actions of people
	Prevailing atmosphere during an incident
	Location of evidence
	Record of criminal activity

Secondary Information

Examples of data the User could **unintentionally** capture that may not be relevant to a police investigation, but is potentially sensitive in nature.


















Operational Policing		Police and Emergency Personnel		Members of the Public	
Police tactics, in-house acronyms and information relating to other incidents		Personal information on police staff and other emergency personnel on scene		Personal and sensitive information on members of the public	
	Radio communications		Visual identification*		Visual identification*
	Intelligence sources		Verbal identification*		Verbal identification*
	Access codes to buildings and electronic devices		Private conversations and comments		Private conversations and comments
	Internal layouts of police buildings		Personnel in a distressed state		People in a distressed state
	Policing acronyms and codes		Information displayed on personal mobile devices		Features of a person's vehicle
	Information displayed on police notebooks as well as on in-car and mobile devices		Shoulder or other identification number		Features within a person's home
	Location information such as a Sat Nav screen		Name badge or ID pass		Features of a person's work place
					People in a state of undress

*See following table on Visual and Verbal Identification

Visual and Verbal Identification





















Examples of sensitive information that could in part or whole lead to the identification of a person.













Identification is the ability to distinguish an individual from another member of a group.

Direct		Indirect	
Unique attribute that could directly identify a person		Strong attribute that could indirectly identify a person	
 Face		 Part of a person's name or a nickname	
 Voice		 General clothing and baggage	
 A person's name		 Uniform and branded clothing	
 Name badge or ID pass		 Hairstyle and beards	
 Email address		 Jewellery	
 Telephone number		 Personalised mobile phone	
 Vehicle number plate		 Tattoos, marks and scars	
		 Pet	
		 Injury	
		 Vehicle or bicycle	














Special Locations




Examples of locations that carry a greater risk of unintentionally recording sensitive information.

Private Home		Hospital		Residential Care		Police Station	
	Details of children whether present or not		Patients in physical distress		Building access codes		Building access codes
	Domestic disorder of property		Personal medical confidentiality		Occupants in a state of undress		Details of police investigations
	Occupants in a state of undress		Patients in a state of undress		Details of vulnerable people whether present or not		Identification of personnel
	Emotionally distressed occupants		Emotionally distressed patients or visitors		Personal medical products		Identification of visitors
	Identification of occupants		Identification of patients, staff or visitors				
	Personal medical products		Location of pharmaceutical products				

Prison		Bank		Place of Worship	
	Building access codes		Building access codes		Intrusion of private contemplation
	Building layouts		Building layouts		Intrusion of private ceremonies
	Identification of personnel		Identification of personnel		Identification of people attending group sessions
	Identification of inmates		Security protocols		
	Security protocols				

Recommendations



 	<p>Ensure that any deployment of BWV is compliant with the DPA18</p>
	<p>Ensure that any deployment of BWV is in line with advice and guidance from the ICO and SCC</p>
 	<p>Ensure standard operating procedures are in place to guide BWV users on when to activate and deactivate a recording</p>
 	<p>BWV users should be aware of their device's potential to capture large amounts of unintended sensitive information</p>
 	<p>BWV users may need to consider ending a recording or temporarily covering the camera or microphone or both in order to minimize the capture of sensitive information</p>
 	<p>Greater discretion may be required when recording in special locations</p>
 	<p>Ensure processes are in place to manage rights for an individual recorded by BWV devices including Subject Access Requests and restriction of personal data</p>

KEY	
	<p>Training points</p>
	<p>Good practice</p>
	<p>Advice</p>



Scenario

An officer with BWV attends a domestic violence incident and records the following information.


Officer driving to incident

Primary Information	
	Radio communications relating to the incident
	Decisions and actions of the BWV User





Secondary Information	
	Radio communications relating to intelligence sources
	Private conversations between officers




Arrives at scene

Primary Information	
	Decisions and actions of the BWV User




Secondary Information	
	Location of private premises
	Private conversations between officers




Enters premises

Primary Information	
	Location of evidence
	Record of criminal activity
	Decisions and actions of the BWV User






Secondary Information	
	Features within a person's home









Attends to victim

Primary Information	
	First account from the victim
	Physical and mental state of the victim
	Decisions and actions of the BWV User





Secondary Information	
	Family picture
	Direct facial identification
	Indirect identification - jewellery



Questions suspect

Primary Information	
 	First account from the suspect
 	Demeanour of the suspect
 	Action of the suspect
 	Decisions and actions of the BWV User






Secondary Information	
	Direct facial identification
	Indirect identification - clothing logo

Leaves premises

Primary Information	
 	Decisions and actions of the BWV User



Secondary Information	
	Radio communications identifying officers
	Indirect identification - parked vehicle
	Officers discussing suspect

2. Consequences of losing BWV data

As covered in Section 1, a BWV device can capture a large amount of sensitive information that may have no evidential value but if mislaid could have a negative impact on members of the public as well as local community relations.

Beyond the obvious loss of potential evidence, mislaid BWV data can have a much wider impact with serious negative consequences for individual police forces, the wider police service or the Criminal Justice System (CJS) as a whole. Significantly the loss of BWV data could not only result in a substantial financial penalty, but also cause an erosion of public trust.

In the age of social media, any unauthorised third party obtaining a BWV recording has the mechanism to instantly share data with a global audience. While any consequences will be largely unpredictable they are unlikely to be positive.








Guidance on reporting breaches is available from the [ICO](#).




Negative impacts of losing BWV data

Examples of how the loss of BWV data could impact the public and policing.

Members of the Public	Police Personnel	Local Policing	National Policing
Invasion of a person's privacy	Compromise the duty of care to personnel	Compromise police investigations	Loss of trust in the CJS
Compromise the safety of witnesses or victims	Loss of confidence in BWV technology	Expose police tactics and compromise the integrity of policing	Reputational damage to the national deployment of BWV
Cause personal distress	Compromise undercover officers	Loss of the community's trust	Reputational damage to data security
Reluctance to assist police		Imposing of substantial financial penalties	Negative media coverage on policing
		Corporate reputational damage to force	Erosion of public trust
		Compromise professional partnerships	
		Risk breaching the DPA18	

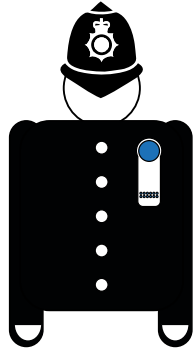
Recommendations

	Complete a Data Protection Impact Assessment (DPIA) to identify the most effective ways to comply with the DPA18 or GDPR
	Consider the wide range of consequences that could result from the loss of BWV data
	Establish processes to ensure that any data breaches are swiftly reported and that potentially negative consequences are minimised
 	BWV users should be aware of the negative consequences of losing their data
 	BWV users should report the loss of their device at the earliest opportunity

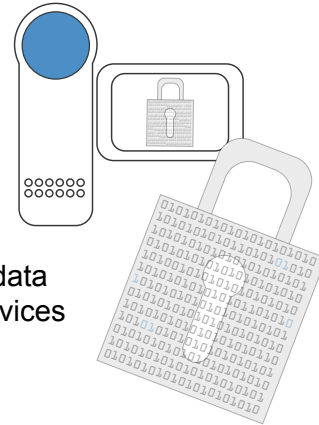
KEY	
	Training points
	Good practice
	Advice

3. Measures to safeguard BWV data

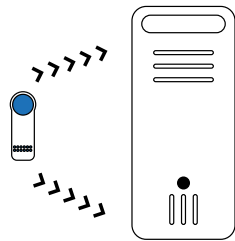
3.1
Physical security of BWV devices



3.2
Protecting data on BWV devices



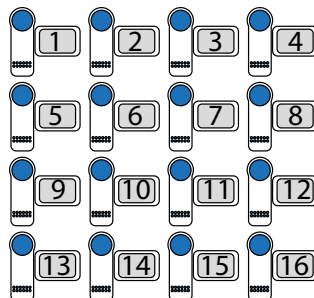
3.3
Transferring data to back office system



3.4
Tagging and organising data



3.5
Asset management of BWV devices



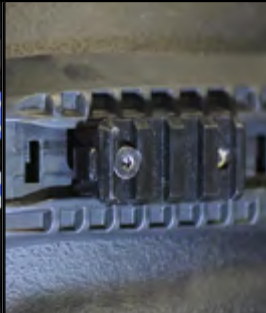



3.1 Physical security of BWV devices



Correctly attaching a BWV device is essential for ensuring that the camera is pointing forward and that the mount is secure. A significant risk to the loss of BWV data is associated with the physical loss of the device itself. Even though a device may be securely attached to an officer’s clothing, it is still possible that a device may be accidentally detached, misplaced, left behind or maliciously removed.












As the examples below show, there are several recommended mounting options for a range of policing roles. See ‘[Technical Guidance for Body Worn Video Devices](#)’ for additional information on mounting.




General Uniformed Policing	Plain Clothed Policing	Armed Policing	
Klick Fast on tactical clothing	Klick Fast on harness	Picatinny rail on helmet or cap	ARC rail on helmet or cap
			

Some policing roles carry a greater risk of losing a BWV device and should be subject to additional safeguards. The table below shows the relative RAG status of risks associated with some common policing roles.

	Property Search	Patrol	Public Order
RISK FACTORS			
Control of the working environment			
Level of hostility			
Physical altercation			
Foot pursuit			
Accessing and exiting vehicle			
Theft of device			

Recommendations

	Whenever possible use recommended mounting options
 	BWV users should check that their device is still attached after a physical altercation or a foot pursuit
 	Notify a colleague if their device has become detached from the mount or is missing
 	If possible, a search should be carried out to locate a lost device
 	Lost devices should be reported as soon as practical
	Instructions should be displayed on the devices so that if found, they can be returned
	BWV users should regularly review their videos to ensure the device is pointing in the correct direction

KEY	
	Training points
	Good practice
	Advice

3.2 Protecting data on BWV devices



In the event that a device, or removable storage media, is either misplaced or stolen a third party may attempt to access the recorded data. All devices should therefore incorporate mechanisms whether physical or electronic to prevent this from happening. However, a balance needs to be struck that ensures sufficient safeguards exist to secure the data while not hampering the effective operational deployment of BWV.

Both the Information Commissioner's Office (ICO) and the Surveillance Camera Commissioner (SCC) recommend encryption as a primary mechanism for keeping data secure on BWV devices. Additional [encryption guidance](#) is published on the ICO's website.

The following tables show the relative RAG status of risk factors associated with common storage media and encryption options.

Storage media options

	Removable Media		Non-removable Media	
	SD or microSD card in open slot	SD or microSD card behind user accessible cover	SD or microSD card sealed in device	Solid state media embedded within device
RISK FACTORS				
Accidental loss of media	●	●	●	●
Interference with data on media	●	●	●	●
Physical damage to media	●	●	●	●
Compromise to continuity	●	●	●	●
OPERATIONAL IMPACTS				
Flexibility of data transfer options ¹	●	●	●	●

¹ This could benefit the provision of mutual aid services

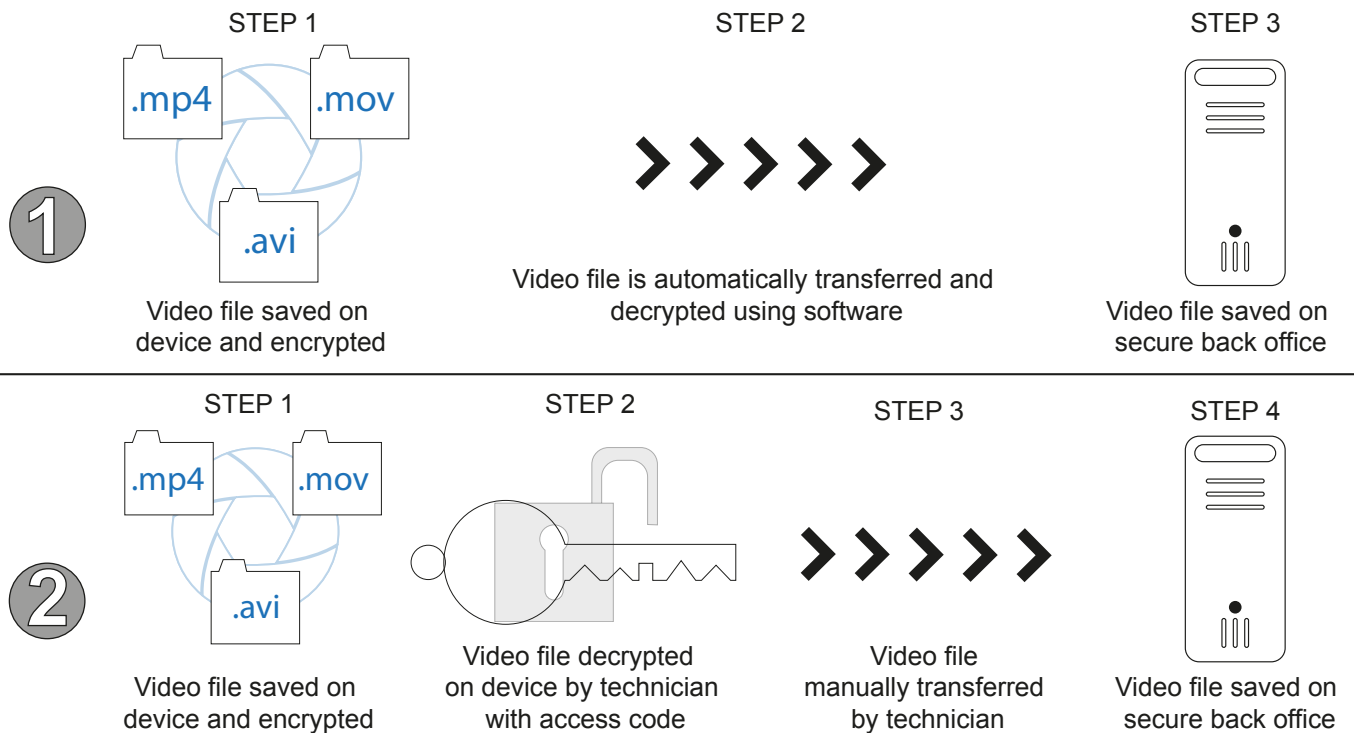
Encryption options

	No Protection	Proprietary Format	Symmetric Encryption	Asymmetric Encryption
	Direct access to data	Data or metadata is scrambled exclusive to a manufacturer	Same access code or key to encrypt and decrypt data	Different access codes to encrypt and decrypt data (public and private keys)
RISK FACTOR				
Data accessible by unauthorised party	●	●	●	●
OPERATIONAL IMPACTS				
Access code management required ¹	●	●	●	●
Sharing data with CJS partners	●	●	●	●
Replay recording on BWV or other mobile device ²	●	●	●	●













¹ Could be a manual or an automated process




² Could involve the use of an app

Two common processes for the encryption and decryption of BWV data are shown below.

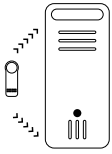


Recommendations

	Non-removable solid state media is preferred
	Encryption is recommended by both the ICO and SCC
	Symmetric encryption should be an AES system
	Asymmetric encryption should be an RSA system
	Decryption of data is best managed automatically by the back office system
	Do not use proprietary formats as this compromises the ability to process and share the data
	Devices with screens should require an access code to replay recorded video
	BWV users should be allocated individual access codes
	Access codes must not be obvious, nor the factory default, nor officer shoulder number
	Access codes should be regularly changed
	Inform the ICO if any personal data is lost
	BWV users should have an appropriate knowledge on how data is securely managed

KEY	
	Training points
	Good practice
	Advice

3.3 Transferring data to back office system



Proper and timely data management should ensure data is transferred off the device to a secure back office system as soon as practical. Normally this will mean by the end of the BWV user’s shift. Another benefit of timely data management is the ability for the User to recall any events or information that need to be associated with the recording through tagging (See Section 3.4).

All recordings should be erased from the device once the data has been transferred to the force’s back office system.







As well as transferring data, connecting to a secure back office system provides the opportunity for devices to have their clocks recalibrated, firmware updated, encryption systems managed or functions reconfigured.




The relative RAG status of risk factors and operational impacts for alternative data transfer methods are shown below.

	Removable Storage Media	Cable¹	Cable¹ and Software	Docking Station and Software
	Data is transferred by physically removing the storage media	Data is transferred via a USB cable only	Data is transferred via a USB cable and dedicated software	Data is transferred via a docking station and dedicated software
RISK FACTORS				
Loss of data				
Compromise to continuity				
Management of data tagging				
Virus infection				
Implementation of encryption				
OPERATIONAL IMPACTS				
Installation and set up				
User input required				
Interoperability				
Update device firmware				

¹ Could also be a secure wireless connection

Recommendations

	Any data transfer process should be automated to minimise user input
	Docking stations should act as the primary method to transfer data as well as recharge and store devices
	Location of docking stations should be secure and accessible
	Devices should as a backup allow for data transfer via a USB cable or a secure wireless connection
	BWV users should be aware of all available methods to transfer data
	BWV users should transfer data as soon as practical

KEY	
	Training points
	Good practice
	Advice

3.4 Tagging and organising data



All video files from BWV devices should have a unique reference. Additionally, the User should be required to manually label or tag each video file with information that relates to its retention period, content and when possible a crime reference. This information is often called business metadata as opposed to technical metadata that the device automatically applies to the video file to ensure playback.

This tagging of data mostly takes place once the video files have been transferred to the back office, but may be done in the field using an app on another mobile device. Regardless of the method employed, files should be tagged as soon as practical while details of the recording are fresh in the User's mind.

Not only does this tagging of data support continuity of evidence, but it helps to ensure its provenance. Furthermore, correctly tagged BWV data can be stored within a structured filing system enabling future search and retrieval.











BWV technical metadata is likely to be consistent for all devices, though the full extent of business metadata required will likely reflect similar processes already in use by individual forces.




Metadata

Common metadata fields are shown in the table below.

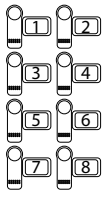
Business Metadata		Technical Metadata
Continuity Information	Incident Information	Video Information
Automatically applied by the BWV device or back office system	Manually applied by the BWV User	Automatically applied by the BWV device
Device reference	Crime reference	Start time and date
Unique file reference	Description of content	Length of recording
BWV user's name or identification	Type of offence	Image resolution
PNC Force identification	Data retention parameters	Frame rate
Associated video files	Operation name	File size
	Free text user comments	Location information such as GPS data

Recommendations

	BWV data should be tagged so it can be organised, searched and retrieved
	Metadata fields and entry options should be standardised wherever possible
	Back office software interface should assist the BWV User with the tagging process
 	Video files should be tagged by the BWV User as soon as practical
 	Data retention parameters should be set as soon as possible
 	A crime reference should be linked to the video file whenever possible
	BWV users should be aware that long recordings may be split into more than one file to improve replay

KEY	
	Training points
	Good practice
	Advice

3.5 Asset management of BWV devices












Asset management generally refers to a systematic process of deploying, operating, maintaining, upgrading and storing devices.

As with other mobile electronic police equipment, effective procedures should be in place to manage BWV assets. These procedures should factor in the BWV User minimising any impact on their operational roles.

Importantly any asset management process should accurately record who a device is assigned to, the location of the device and its operational status.

Recommendations

	Personal issue of BWV devices has proven to be beneficial for many police forces
	Unique asset reference should be visible on all devices
	Status records should be maintained for all devices such as; in use, charging, faulty or under repair
	Devices should be stored securely when not in use
	Near Field Communication (NFC) and Radio Frequency Identification (RFID) technologies can benefit asset management
	BWV users should be aware of their role and responsibility for managing their devices

KEY	
	Training points
	Good practice
	Advice

4. Distributing BWV data

At times, it will be necessary to provide copies of BWV recordings to third parties either for policing purposes such as evidence for partner agencies within the criminal justice system or through a Subject Access Request (SAR) from a member of the public. As mentioned in Section 1 BWV devices can capture large amounts of visual and audio data some of which may need to be redacted prior to distribution.

Redaction covers the editing, censoring or obscuring of those parts of a recording that could unwittingly reveal sensitive information, expose police tactics or compromise operational strategies. On a practical level this could mean trimming the length of the original recording, concealing or masking specific visible objects and actions as well as removing metadata and muting parts of the audio track.



























Once BWV data has been appropriately redacted it is important to have different delivery methods to satisfy the requirements of the recipient. Regardless of delivery method any personal or sensitive data must be protected while in transit.




4.1 Sharing data for policing purposes

As part of a police investigation it is likely that BWV data will need to be shared with law enforcement partner agencies and the Crown Prosecution Service (CPS). Also there may be a need to provide BWV data as evidence for civil prosecutions, as training material or to the Media either as part of a public appeal or for TV documentaries. Redaction requirements will naturally vary from case to case with the responsibility likely to rest with the senior investigating officer.

Redaction considerations

Examples of what should be considered for redaction when releasing BWV data in some typical circumstances.

Court Compilation		Training		Public Domain	
BWV recording to be shown in court		BWV recording replayed during police training sessions to add realism		BWV recording released into the public domain to progress an investigation	
 Identification of people not connected with the incident		 Identification of victim or witnesses		 Identification of a person other than the primary subject/s	
 Information that may compromise the safety of a person		 Additional personal or sensitive information such as medical records		 Identification of any emergency personnel	
 Any part of the recording not agreed with the defence and prosecution		 Information that may negatively impact a police investigation		 Exposure of police tactics or operational knowledge	
 Any part of the timeline not required		 Any part of the timeline not required		 Any part of the timeline not required	
				 Original file name	
				 Business metadata	

KEY					
	Audio		Visual		Metadata

4.2 Releasing data for Subject Access Requests (SAR)

A Subject Access Request (SAR) is simply a request made by or on behalf of an individual (the Data Subject) for their personal data as well as other supplementary information. Entitlement for this information is either under Part 3 of the Data Protection Act 2018 (DPA18) for data being processed for the prevention and detection of crime or article 15 of the General Data Protection Regulation (GDPR) for other data.

While a Data Subject is entitled to their personal data they are not entitled to another person's personal data especially if this could cause that person harm. It is not possible to restrict or control how the Data Subject shares the information provided to them. With this in mind it is important to presume that the information could be posted on Social Media and quickly reach a potentially global audience.

Further information on SARs is available on the ICO website for [DPA18](#) or [GDPR](#). These links also contain guidance on what supplementary information should be disclosed to the Data Subject.

Once general decisions have been made regarding what data should be disclosed it will be necessary to redact the data that shouldn't be disclosed. While some aspects of the redaction process are straightforward, there will be those that require additional consideration and justification to ensure compliance. Maintaining a record of these decisions should be considered good practice.

Personal data can be represented visually or within the audio track and redacting this data requires certain techniques to avoid unwitting disclosure. Technically redacting visual and audio data can be complex but the guidance below is designed to simplify the process yet allow compliance with data legislation. Actual application of this information may vary on a case by case basis.

Redacting visual and audio data requires specialist software such as that used for professional video production, video forensics or provided with a BWV back office. While professional software requires training and expertise to operate as well as costly hardware, redaction suites provided as part of a BWV back office tend to be easy to use and can use cloud based processing power. Any of this software used in conjunction with this guidance should enable a Data Controller to be compliant with data protection legislation.

Checklist for Data Controller

Considerations when processing a Subject Access Request.






Consideration	Reason	Details
Verify identity of Data Subject	Avoid disclosing personal data to the wrong person	<ul style="list-style-type: none"> - Recent photograph - Clothing description - Voice sample
Obtain contact details of Data Subject	Understand nature of the request and manage expectations	<ul style="list-style-type: none"> - Purpose of request - Explain disclosure policies - Timescales
Locate all BWV data	Data Subject's personal information may appear in more than one BWV recording	<ul style="list-style-type: none"> - Time and date of event - Location - BWV user's name or ID - Type of event
Impact on policing	Disclosure of data could prejudice security	<ul style="list-style-type: none"> - Prevention & detection of crime - Investigation & prosecution of crime - Public or National security
Impact on partner agencies	Agreement on data disclosure for partner agency personnel	<ul style="list-style-type: none"> - Blue light services - Civil enforcement - Health & Community care
Impact on third parties	Internal policy for disclosing third party data either with or without consent	<ul style="list-style-type: none"> - Subject's family members - Subject's friends and associates - Any personnel in their workplace
Location where recording took place	Increased likelihood of third party personal data in some circumstances	<ul style="list-style-type: none"> - Hospital - Schools - Residential care - Places of worship
	Decreased expectation of privacy in some circumstances	<ul style="list-style-type: none"> - Shopping centres - Transport hubs - The High Street
Potential circulation of data	Likelihood that redacted video will be further circulated by the Data Subject	<ul style="list-style-type: none"> - Mainstream media - Social media platforms - Open source video platforms



The following examples show images and tables listing video and audio information that could lead to the identification of a person.


Example A:

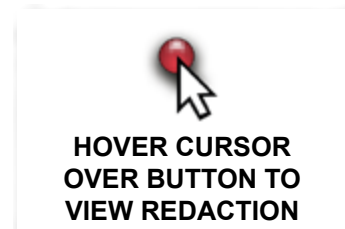
Subject 2 is recorded during a Stop and Search and requests a copy of the recording.



Subject 1		
	Facial identification	
	Clothing - baseball cap	
	Clothing - jacket	
	Jewellery - necklace	
	Voice identification of subject	

Subject 3		
	Facial identification	
	Clothing - jacket	

BWV User		
	Subject's email address and telephone number	












Subject 1

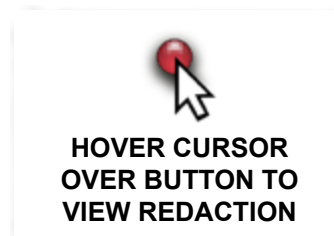
Subject 2



Subject 3



Subject 1		
	Facial identification	
	Clothing - trousers	
	Jewellery - ring	
	Distinct mobile phone ring tone	
	Voice identification of subject	
	Subject's mother's home address	

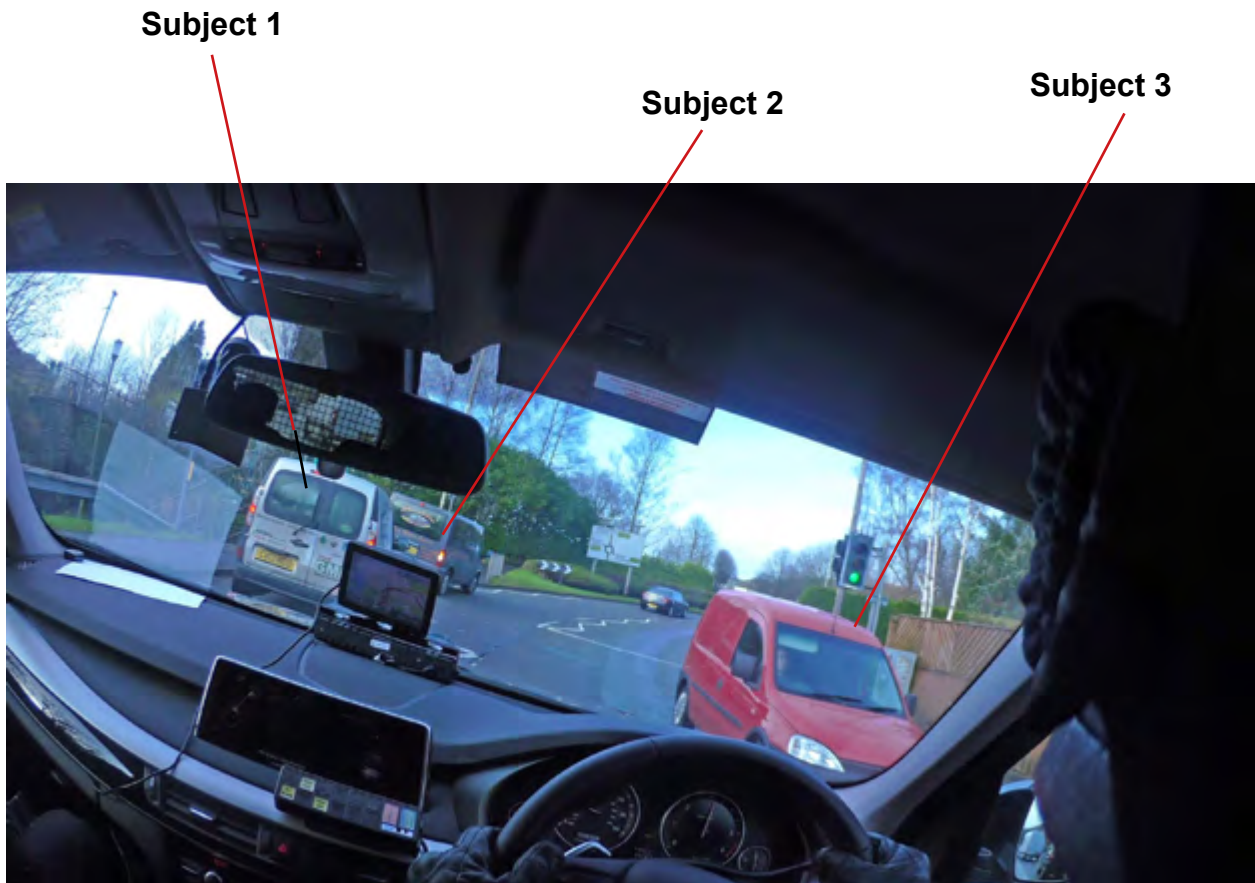
Subject 3		
	Facial identification	
	Clothing - handbag	
	Clothing - footwear	







BWV User		
	Radio communications identifying witness	
	Private conversation between officers	


Example B:




Subject 3 is recorded by an officer in a passing police car and requests a copy of the recording.

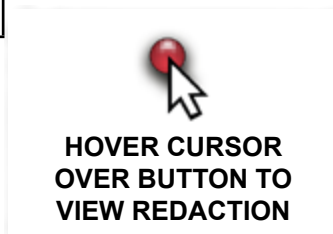


Subject 1		
	Company logo	
	Number plate	

BWV User		
	Private conversations between officers	
	Identification of officers	

Subject 2		
	Company logo	

In Car		
	Identification of intelligence sources	
	Location of destination on Sat Nav	
	Details of incident on display	



4.2.1 Visual data redaction

This involves the masking of people and objects appearing in the video. One characteristic of BWV recordings is that the camera or subjects are rarely static so the position of any masks will likely require altering throughout the duration of a recording. This is especially true for head mounted cameras used by Firearms Officers.

Disclosure requirements

Visual data related to the Data Subject that should be disclosed.

Type	Examples
Direct identifying features	- Facial features - Name badge
Indirect identifying features	- Clothing and jewellery - Tattoo
Related visual information	- Contact details visible on a screen - Location information on Sat Nav
Identified vehicle	- Number plate - Company branding
Directly attributed comments about the Data Subject	- Officers discussing the Data Subject - Radio communications about the Data Subject

Redaction considerations

Visual data that does not need to be disclosed to the Data Subject.

Type	Example
Data Subject's indirect identifying features either adjoining or overlapping third party data	<ul style="list-style-type: none"> - Person walking behind Data Subject - Child held close to Data Subject
BWV User's indirect identifying features	<ul style="list-style-type: none"> - Jewellery - Scars and tattoos - Badge number
Other Blue Light personnel	<ul style="list-style-type: none"> - Firefighter attending an incident - Medic working in a hospital
Other partner agencies personnel	<ul style="list-style-type: none"> - Social worker attending an incident - Highways officer managing traffic
Third party associated with the event	<ul style="list-style-type: none"> - Witness - Victim
Third party not associated with the event	<ul style="list-style-type: none"> - Person walking around the incident - Driver in slowing vehicle
Third party known to the Data Subject	<ul style="list-style-type: none"> - Member of the family - Neighbour
Location information	<ul style="list-style-type: none"> - House and street names - Local landmarks
Vehicle identification	<ul style="list-style-type: none"> - Number plates - Company branding
General information	<ul style="list-style-type: none"> - Contextual data - Time and date in BWV recording

Redaction techniques

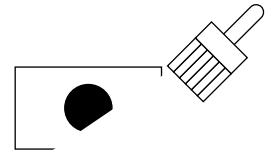
Technical methods that can be applied to redact video data.

Visual examples can be in seen in the following images.

Technique	Acceptable application	Notes
Mask shape	Fixed shapes such as oblongs, circles and ovals that can be scaled and rotated	Free form shapes or polygons are complex and time consuming for little benefit
Mask overlap	Mask can be larger than feature or object so it does not require alteration under small movements	Balance required to ensure no or limited redaction of Data Subject
Mask fill (solid)	Use of an opaque colour to completely obscure data	Most secure and consistent method to obscure data
Mask fill (blurring & pixilation)	Ensure level is consistent and effective throughout a clip	Greater caution necessary to ensure effective redaction, though helps to retain a degree of context to the event
Single mask (general)	Best to cover the entire body rather than just the head	It may be possible to indirectly identify third party through unique clothing, jewellery or tattoos
Single mask (close to Data Subject)	Some minimal redaction of the Data Subject is allowed to avoid disclosure of other personal data	A common example is people not involved with the incident walking behind the Data Subject
Single mask (gesticulations)	Fast and erratic arm movements by the Data Subject can be redacted to avoid disclosure of third party data	Highly complex task to redact constantly changing subject for little benefit to the Data Subject
Dual mask (nearby)	If two objects are close together then a single mask can be applied rather than two separate masks	A common example is a parent with a child
Dual mask (apart)	If two objects are apart then two separate masks should be applied	A common example is two unconnected witnesses to an event
Inverse mask	If three or more objects in a scene need redacting then inverse redaction can be applied	A common example is the Data Subject amongst a crowd of people
Automation	Likely to still require some manual input to ensure effective throughout	Less effective when an object's motion is fast and erratic

Applying the Mask

Suggested Method



This mask uses a simple ellipse shape tool adjusted to provide a small buffer around the person

The person's clothes are covered so could not identify them



Occasional adjustments to the position of the mask may be necessary as the video plays

Small movements of the person or the BWV device would not reveal any personal information

Alternative Methods

This mask uses a simple ellipse shape tool adjusted close to the person's head

The person's clothes are not covered so could indirectly identify them



Frequent adjustments to the size and position of the mask will be necessary as the video plays

Any movement of the person or the BWV device could reveal personal information

This mask uses a complex free form shape tool adjusted close to the person

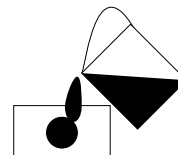
The person's clothes are covered so could not identify them



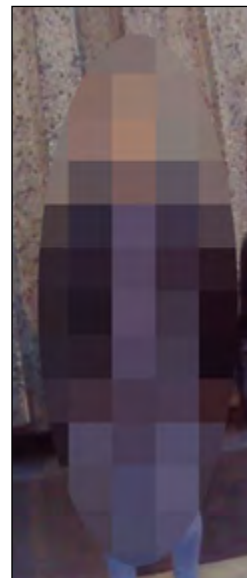
Frequent adjustments to the shape and position of the mask will be necessary as the video plays

Any movement of the person or the BWV device could reveal personal information

Filling the Mask

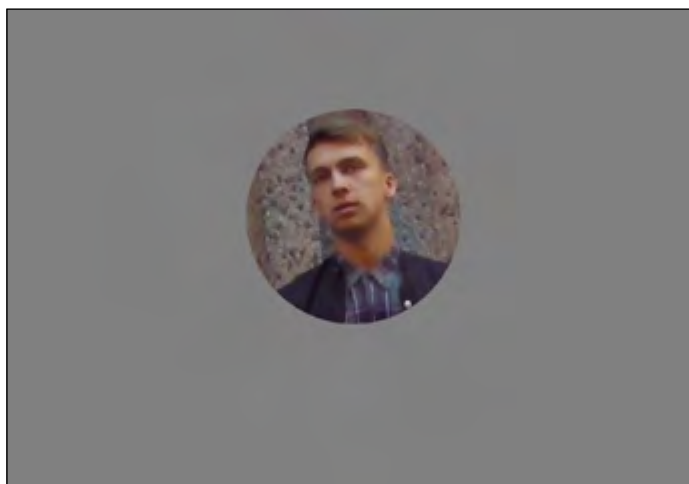


Solid fill of the mask ensures a low risk of disclosing personal information or features that could indirectly identify a person

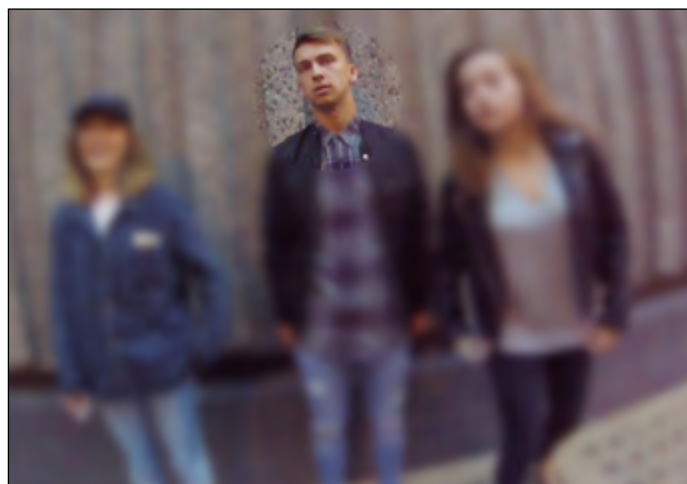


Both blurring (left) and pixelation (right) present a higher risk of disclosing personal information and features that could indirectly identify a person. However these methods can provide visual context to the scene

Inverse redaction



Using solid fill only shows the Data Subject's personal information and does not disclose features that could indirectly identify other people in the scene



Using blur shows the Data Subject's personal information, but there is a higher risk of disclosing features that could indirectly identify a person. However there is greater visual context to the scene

4.2.2 Audio data redaction

This involves the muting of voices and sounds on the video's audio track. Identifying a person off camera by their voice is a difficult task and requires a degree of caution especially when voices are raised.

Disclosure requirements

Audio data that should be disclosed to the Data Subject.

Type	Example
Data Subject's voice	Comments made during discussion with BWV User
BWV User's voice	Police officer's comments when talking with Data Subject
Comments regarding and linked to Data Subject	Off screen discussion between police officers
Communications regarding and linked to Data Subject	Radio communications disclosing Data Subject's address or criminal record

Redaction considerations

Audio data that should not be disclosed to the Data Subject.

Type	Example
Data Subject's voice when disclosing third party data	Data Subject talking about a person and mentioning their phone number
BWV User's voice when disclosing third party data	BWV User obtaining phone number from witness when Data Subject is out of earshot but still visible
Non identifiable voices	Shouted comments made by a person off camera
Blue Light personnel voices	Paramedics discussing treatment of Data Subject
Partner agencies personnel voices	Social worker discussing a child's welfare
Third party audio associated with the event	Victim discussing actions of the Data Subject
Third parties not associated with the event	Local person walking past and talking to a friend
Communications audio	Chatter from Officer's radio providing the address of a third party

Redaction techniques

Technical methods that can be applied to redact audio data.

Technique	Acceptable application	Notes
Mute indicator	A visible or audible indicator should be present when audio has been redacted	Enables the Data Subject to distinguish between audio redaction and silence
Audio waveform	Cueing audio is difficult, but can be improved with a waveform generator	Reducing video speed for cueing does not affect visual data, but makes audio data intelligible
Mute by word	When only one voice can be heard individual words can be muted	Best applied when most words remain unredacted
Mute by comment	When multiple words need redacting from a comment	Ensures that remaining audio is intelligible
Subtitles	Can be used as alternative to muting when multiple voices on audio track	Should only be used when audio is clear and not open to interpretation

4.2.3 Output video and audio data



















It is the responsibility of the Data Controller to ensure that the Data Subject's request is completed within a calendar month and that the data disclosed or redacted is compliant and justifiable.

Output Considerations

Points to consider when providing the redacted product to the Data Subject.








Consideration	Details
Control of data	No constraints can be applied to the Data Subject's use of the product such as not posting on Social Media platforms
Multiple videos	Output can comprise a number of video clips
Check redaction	Perform frame by frame analysis of the video to ensure redaction has been successful especially where fast motion exists
Non reversible redaction	It should not be possible to reverse any of the redaction actions
Video compression	It may be necessary to compress the video to reduce file size, though this should not affect disclosure of the Data Subject's personal data
Encryption	Personal data should be encrypted when in transit either electronically or by post
Provision of redacted recording	Can be provided via a secure hyperlink, email attachment and by post




The relative RAG status of risk factors and operational impacts for alternative data distribution methods are shown below.

	CD/DVD (sent by post or courier)	CD/DVD (delivered by staff member)	Electronic data transfer or access ¹
RISK FACTORS			
Loss of data in transit			
Compromise to continuity			
Control over distribution			
Apply technical security measures such as encryption			
OPERATIONAL IMPACTS			
Delivery cost			
Time taken			

¹ Includes secure hyperlink

Recommendations

	Subject Access Requests should be dealt with through an established process
	Ensure compliance with the DPA18
	Record justifications for redacting and disclosing personal and sensitive data
	Contact Data Subject to better understand the nature of the request and manage expectations regarding the output
	Apply a consistent approach to redaction, though each case may require individual consideration
	A frame-by-frame review of the redacted recording should be performed to ensure compliance with requirements
	BWV users should be aware that people appearing in their recording can request a copy

KEY	
	Training points
	Good practice
	Advice

ISBN 978-1-78655-627-1