Home Offi

Safeguarding Body Worn Video Data

Published October 2016

Publication No. 076/16

Author: Toby Nortcliffe

Safeguarding Body Worn Video Data

Publication No 076/16

ISBN 978-1-78655-141-2

FIRST PUBLISHED 2016

Home Office -

Centre for Applied Science and Technology

Sandridge

St Albans

AL4 9HQ

United Kingdom

TELEPHONE:	**+44 (0)1727 816400**
FAX:	**+44 (0)1727 816233**
E-MAIL	**cast@homeoffice.gsi.gov.uk**
WEBSITE:	**www.homeoffice.gov.uk/cast**

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 2016 suggest that there will be over 55,000 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 Centre for Applied Science and Technology (CAST), the Information Commissioner and the Surveillance Camera Commissioner to produce this document on safeguarding data from BWV cameras. The purpose of this document is to prevent data loss in order to protect the public whilst ensuring operational effectiveness of this relatively new technology. 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 specification in order to achieve the best evidence possible.”

Andy Marsh

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.

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.

Other publications that complement this guidance are:

Technical Guidance for Body Worn Video Devices - CAST, October 2016

Encryption guidance - Information Commissioner's Office, March 2016

CCTV Code of Practice - Information Commissioner's Office, May 2015

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 Sharing and redacting data
    - 3.6 Asset management of BWV devices

KEY			
🎙	Audio	🟦	Good practice
🎞	Visual	💬	Advice
MD	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 likely to also 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 cause considerable intrusion into a person's privacy at a time of vulnerability. An obvious form of intrusion that could cause considerable harm is the unintentional identification of a person.

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 certain special locations such a hospital 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 over 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.

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

🎓 🟦	BWV users should be proactive in informing people when they are being video recorded and that this includes audio
💬	Ensure that any deployment of BWV is compliant with advice provided by both the Information Commissioner's Office and the Surveillance Camera Commissioner
🎓 💬	Standard Operating Procedures should be in place to guide BWV users on when to activate and deactivate a recording
🎓 💬	BWV users should be aware of their device's potential to capture large amounts of unintended sensitive information
🎓 🟦	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
🎓 🟦	Greater discretion may be required when recording in special locations
🎓 💬	Ensure processes are in place to manage Subject Access Requests from individuals who are recorded by BWV devices

KEY	
🎓	Training points
🟦	Good practice
💬	Advice

Scenario

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

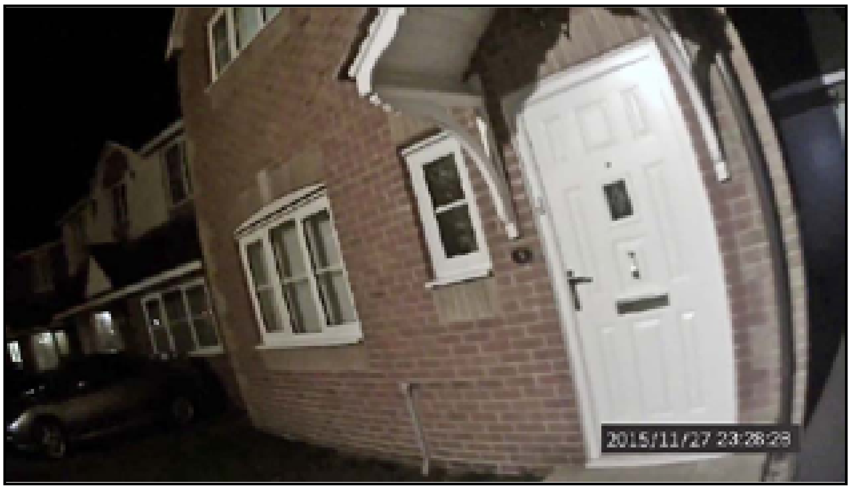
Officer driving to incident

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

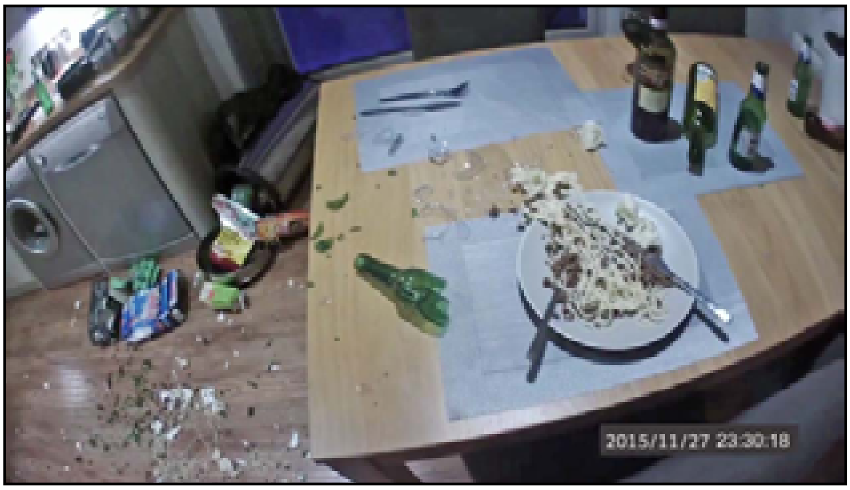
Primary Information	
🎙 🎞	Decisions and actions of the BWV User



Secondary Information	
🎙 🎞	Location of private premises
🎙	Private conversations between officers

Enters premises

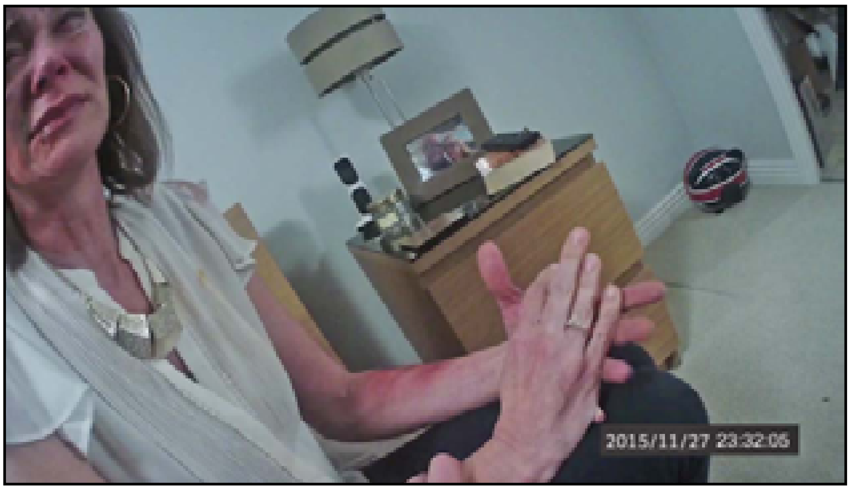
Primary Information	
🎞	Location of evidence
🎤 🎞	Record of criminal activity
🎤 🎞	Decisions and actions of the BWV User



Secondary Information	
🎞	Features within a person's home

Attends to victim

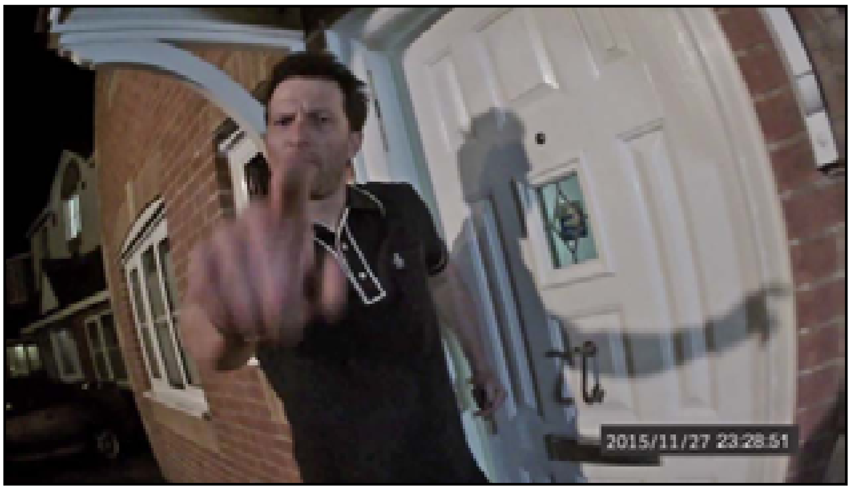
Primary Information	
🎤	First account from the victim
🎤 🎞	Physical and mental state of the victim
🎤 🎞	Decisions and actions of the BWV User



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



2015/11/27 23:28:51

Secondary Information	
🎞	Direct facial identification
🎞	Indirect identification - clothing logo

Leaves premises

Primary Information	
🎙 🎞	Decisions and actions of the BWV User

2015/11/27 23:29:24

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. Furthermore once a BWV recording has hit the social networks removing it is close to impossible.

Negative impacts of losing BWV data

Examples of how the loss of BWV data could impact on a number of levels.

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 Data Protection Act	

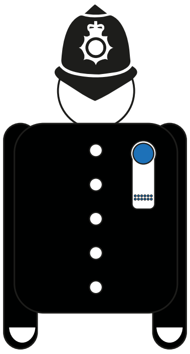
Recommendations

🟦	Complete a Privacy Impact Assessment (PIA) to identify the most effective ways to comply with data protection obligations
💬	Consider the wide range of consequences that could result from the loss of BWV data
🟦	Establish processes to ensure that any data losses 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

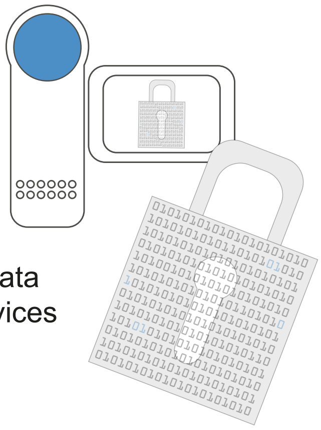
KEY	
🎓	Training points
🟦	Good practice
💬	Advice

3. Measures to safeguard BWV data

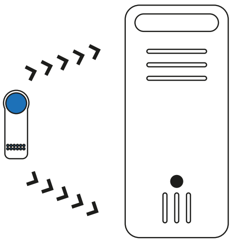
3.1
Physical security of BWV devices



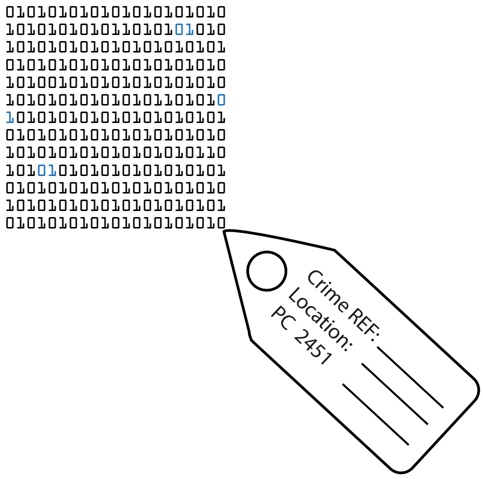
3.2
Protecting data on BWV devices



3.3
Transferring data to back office system

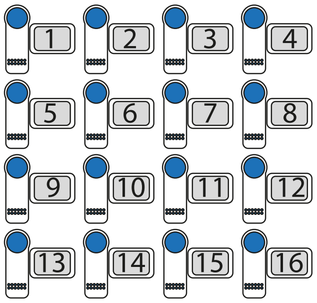


3.4
Tagging and organising data



3.5
Sharing and redacting data

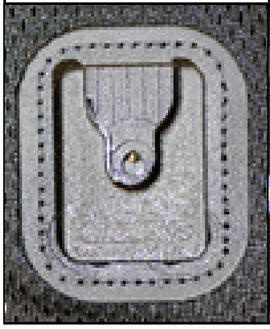
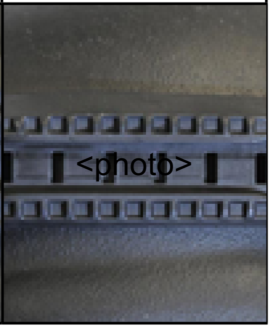
3.6
Asset management of BWV devices



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.

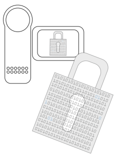
	Property Search	Patrol	Public Order
RISK FACTORS			
Control of the working environment	🟢	🟠	🔴
Level of hostility	🟢	🟠	🔴
Physical altercation	🟢	🟠	🔴
Foot pursuit	🟢	🔴	🟠
Accessing and exiting vehicle	🟢	🟠	🟠
Theft of device	🟢	🟠	🔴

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 recordings should be regularly reviewed to ensure that 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

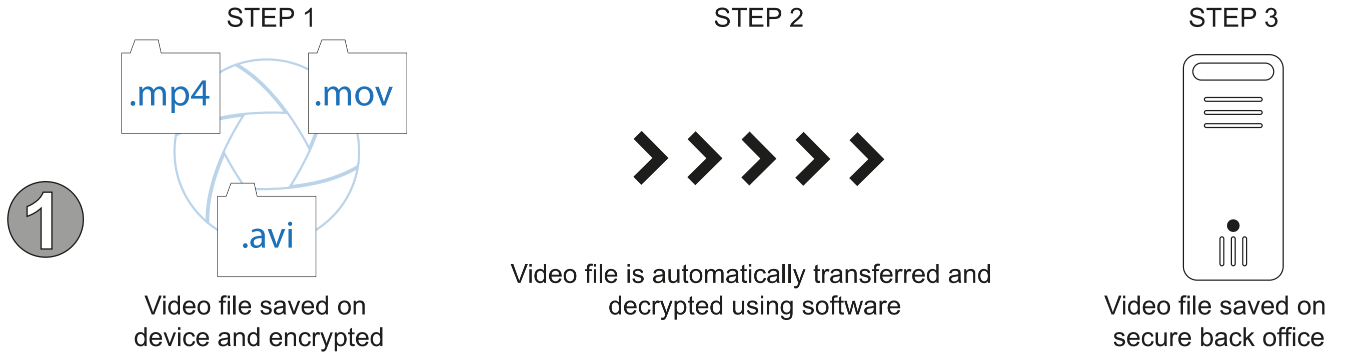
Encryption options

	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.



STEP 1

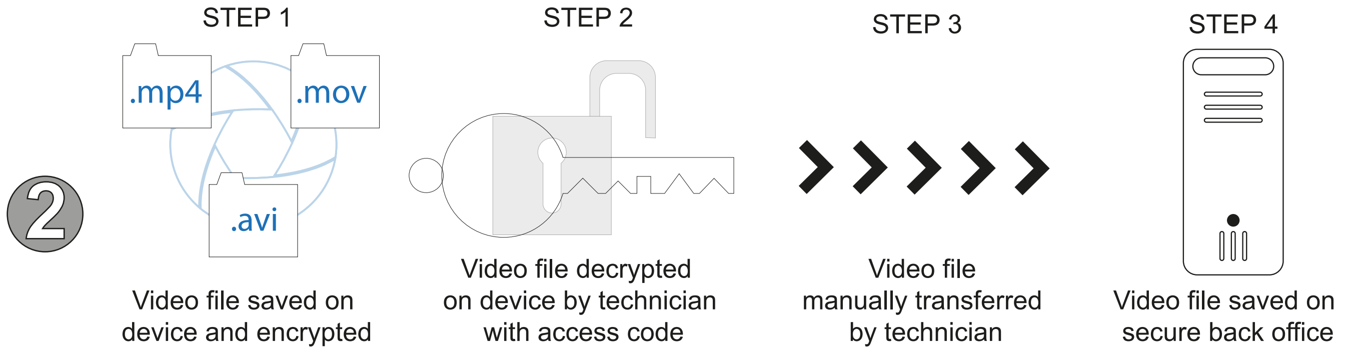
Video file saved on device and encrypted

STEP 2

Video file is automatically transferred and decrypted using software

STEP 3

Video file saved on secure back office



STEP 1

Video file saved on device and encrypted

STEP 2

Video file decrypted on device by technician with access code

STEP 3

Video file manually transferred by technician

STEP 4

Video file saved on secure back office

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.

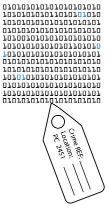
	Removable Storage Media	**Cable**	**Cable and Software**	**Docking Station and Software**
	Data is transferred by physically removing the storage media	Data is transferred via a USB cable only	Data is transferred via a USB cable and dedicated software	Data is transferred via a docking station and dedicated 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	🔴	🔴	🟢	🟢

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 allow for data transfer via USB cable as back up
🎓	BWV users should be aware of how to transfer data using both a docking station and a USB cable

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.

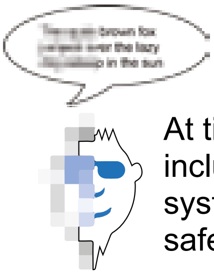
Business Metadata		**Technical Metadata**
Continuity Information	**Incident Information**	**Video Information**
Automatically applied by the BWV device or back office system	Manually applied by the BWV User	Automatically applied by the BWV device
Device reference	Crime reference	Start time and date
Unique 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 Sharing and redacting data



At times, it will be necessary to provide copies of BWV recordings to third parties. This includes partner agencies within law enforcement or those within the criminal justice system as a whole such as the Crown Prosecution Service (CPS). Responsibility for safeguarding this data resides with the police until it has been passed to the agency.

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

	CD/DVD (sent by post or courier)	CD/DVD (delivered by staff member)	Electronic data transfer or access
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	🔴	🔴	🟢

A third party could also be in the public domain, such as a person requesting data held on them through a Subject Access Request as permitted under the Data Protection Act 1998, or to the Media as part of a public appeal, or as evidence for a civil prosecution. In these and some other circumstances it is likely that the recording will need to be redacted.

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 (see Section 1). On a practical level this could mean trimming the length of the original recording, concealing specific visible objects and actions as well as removing metadata and muting parts of the audio track. Although pixelation or blurring may be the obvious method for concealing information, solid masking tends to be more robust. If more than one recording covers an incident then it is important to ensure that redaction is applied consistently.

While the redaction of a document and a photograph is straightforward, this is not the case with a video (audio visual) recording. Any redaction of BWV recordings requires specialist software and appropriately trained personnel.

Redaction considerations

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

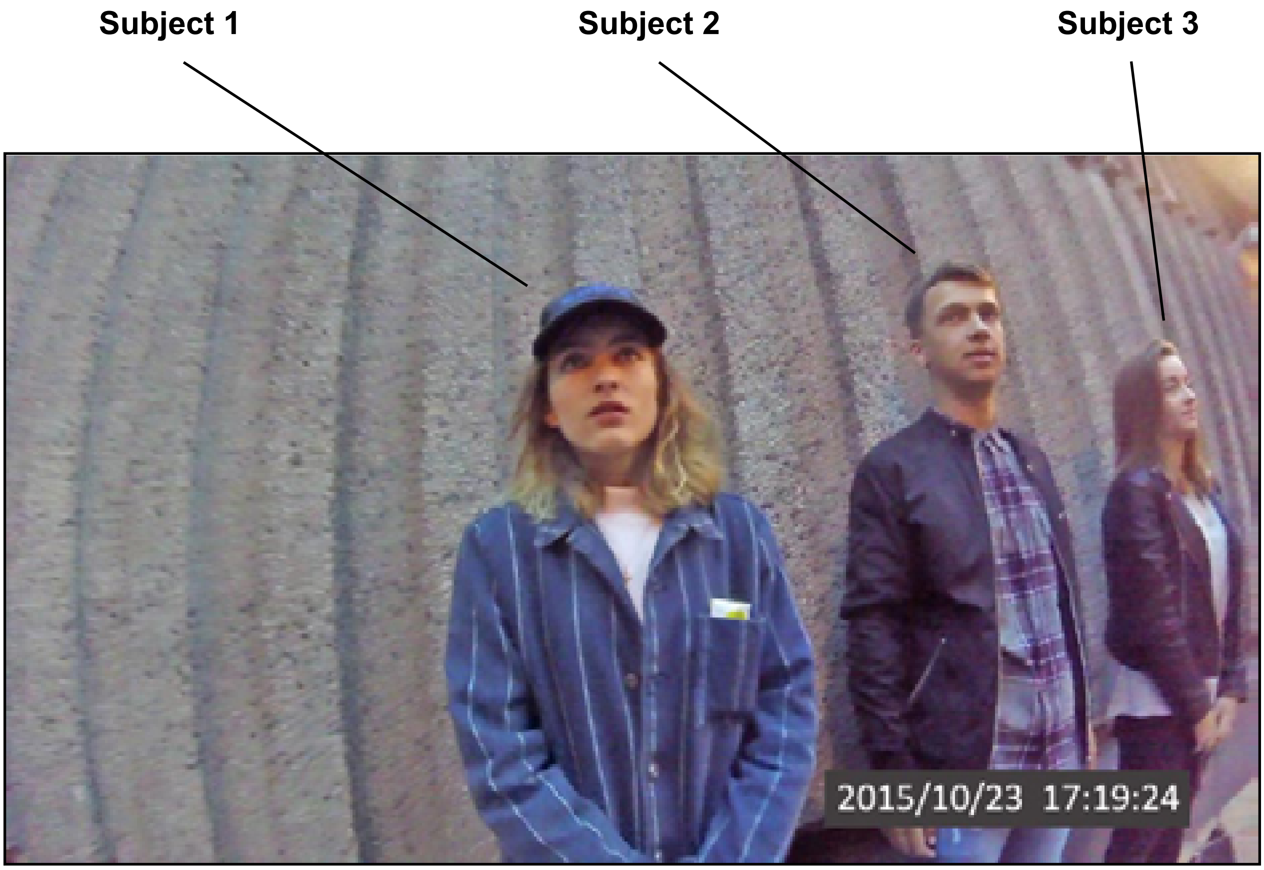
Subject Access Request (SAR)	**Court Compilation**	**Training**	**Public Domain**
Under section 7 of the DPA, people have the right to request personal data an organisation holds about them.	BWV recording that is to be shown in court	BWV recording that is replayed during police training sessions to aid realism	BWV recording that is released into the public domain to progress an investigation
🎙 🎞 Identification of people other than the requester	🎙 🎞 Identification of people not connected with the incident	🎙 🎞 Identification of victim or witnesses	🎙 🎞 Identification of a person other than the primary subjects
🎙 🎞 Identification of emergency personnel	🎙 🎞 Information that may compromise the safety of a person	🎙 🎞 Information that may affect a police investigation	🎙 🎞 Identification of any emergency personnel without their consent
🎙 🎞 Exposure of police tactics or operational knowledge	🎙 🎞 Any part of the recording not agreed with the prosecution	🎙 🎞 Any part of the timeline not required	🎙 🎞 Exposure of police tactics or operational knowledge
🎞 Any piece of recording the requester does not appear in	🎙 🎞 Any part of the timeline not required		🎙 🎞 Any part of the timeline not required
MD Original file name			MD Original file name
MD Business metadata			MD Business metadata

KEY	
🎙	Audio
🎞	Visual
MD	Metadata

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

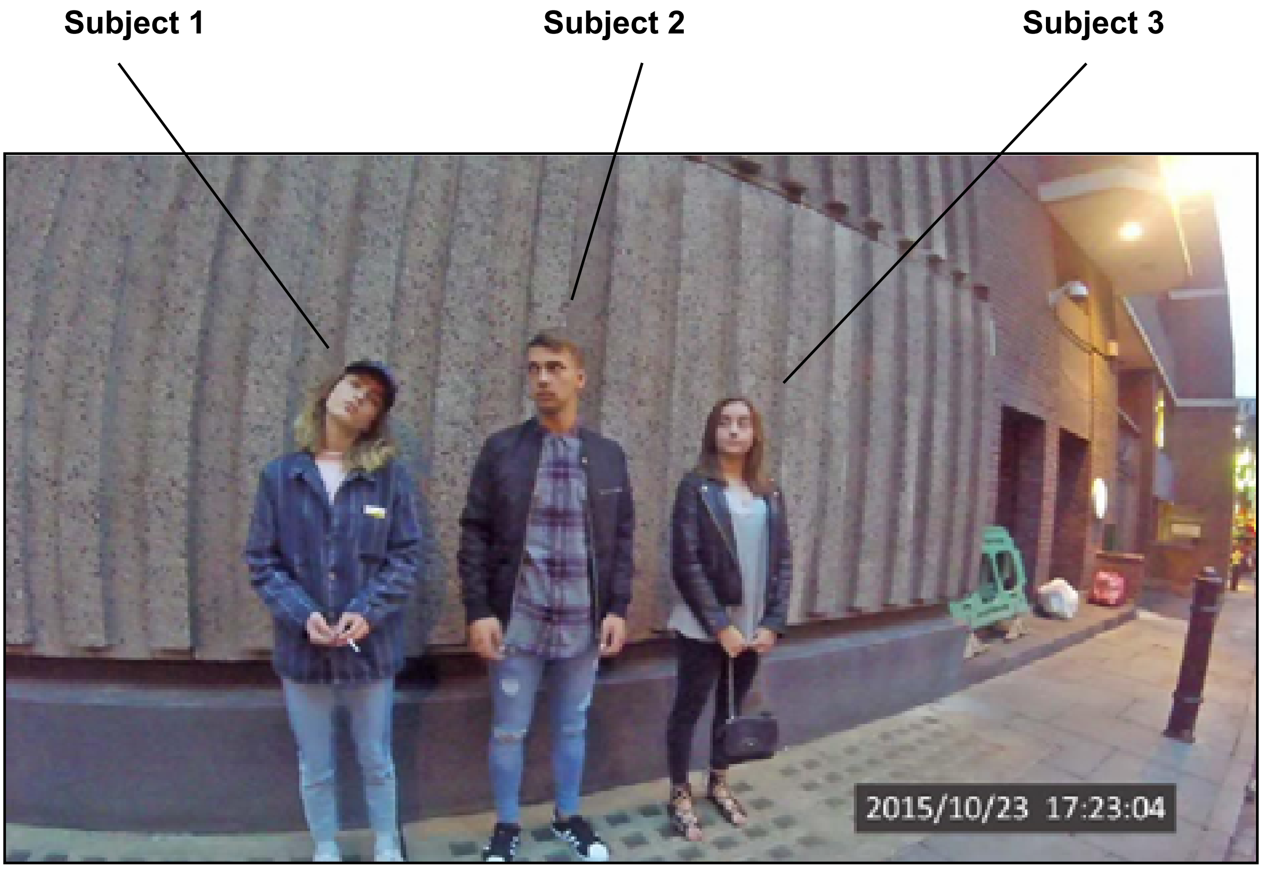
Example A:

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's email address and telephone number

Subject 3	
🎞	Facial identification
🎞	Clothing - jacket



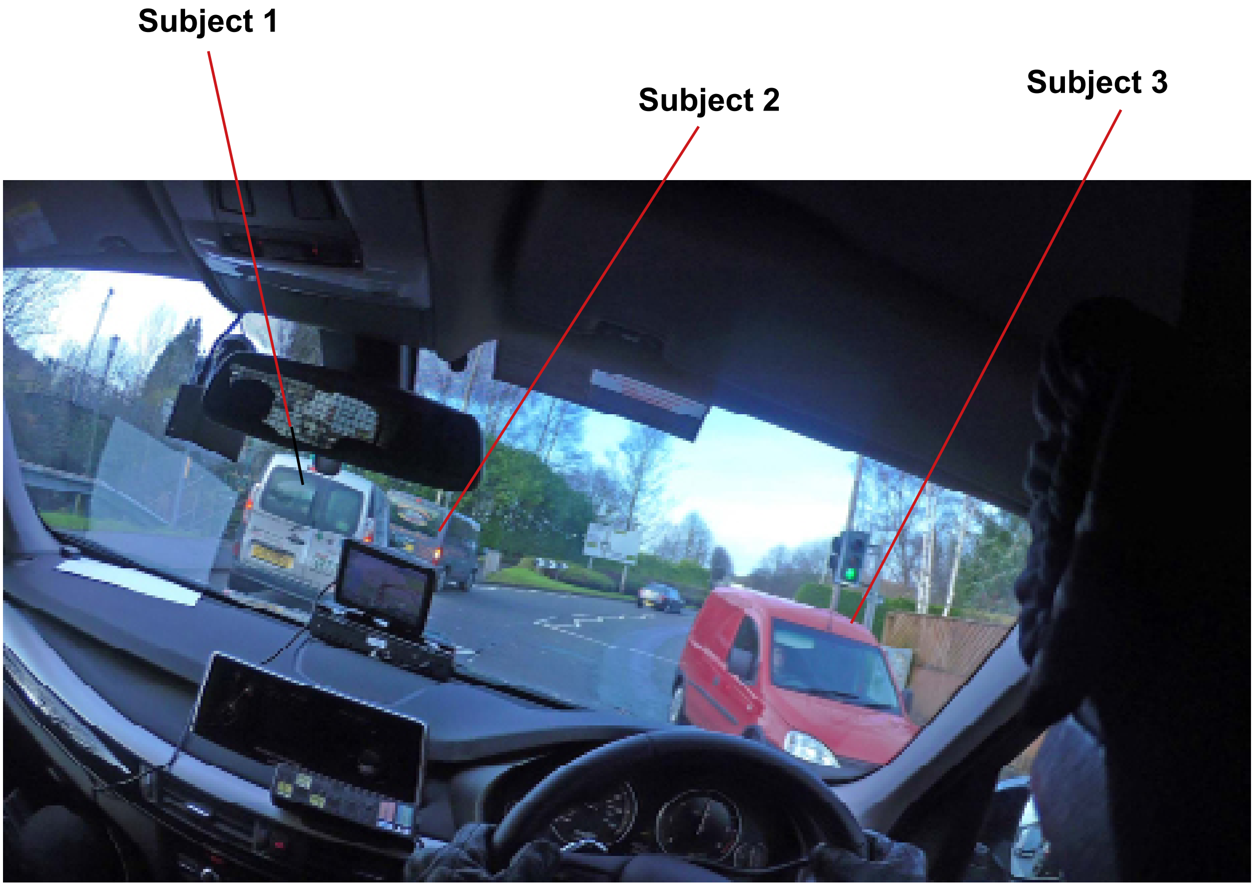
Subject 1	
🎞	Facial identification
🎞	Clothing - trousers
🎞	Jewellery - ring
🎤	Distinct mobile phone ring tone
🎤	Voice identification of subject
🎤	Subject's email address and telephone number

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

Subject 2	
🎞	Company logo

BWV User	
🎙	Private conversations between officers
🎙	Identification of officers

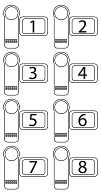
In Car	
🎙	Identification of intelligence sources
🎞	Location of destination on Sat Nav
🎞	Details of victim on PNC display

Recommendations

□	Subject Access Requests should be dealt with through an established process
💬	Ensure compliance with the Data Protection Act
□	Redaction of BWV recordings requires specialist software and appropriately trained personnel
□	Detailed edit lists should be provided to personnel performing the redaction
□	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

3.6 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 BWV assets

KEY	
🎓	Training points
□	Good practice
💬	Advice

ISBN 978-1-78655-141-2