Data Protection Impact Assessment for the use of

Body Worn Video Cameras (BWV)



Data Protection Impact Assessment BWC Introduction

University of Worcester Security Staff carry body worn video cameras (BWV.) The cameras are worn overtly by uniformed staff. This equipment has been introduced in many Universities and Local Authorities in order to deter and detect crime and anti-social behaviour. The cameras will not normally be turned on and will only be activated when the officer is responding to an incident, any activation will be announced. The use of these cameras will be in accordance with the Universities CCTV Policy, relevant legislation including GDPR and the UK Data Protection Act 2018, the Information Commissioners PIA codes of practise, the Surveillance Camera Commissioners Principles and best practice.

The BWV management and retention IT software used by the University of Worcester are supplied by CEESC and is the same equipment supplied widely to police forces and other agencies that deploy public facing staff in potential conflict situations.

It is widely known that citizens, going about their daily lives, are likely to have their movements and identity captured on a myriad of surveillance systems and of paramount importance is the need to mitigate any privacy risks and issues.

This Data Protection Impact Assessment has been written to explore these issues and in particular to explain:

- The rationale for the University of Worcester introducing and using this technology.
- The legality behind its use.
- The likely operational circumstances when uniformed staff may use it.
- The key privacy issues and risks and provides an explanation as to how the organisation mitigates them.
- How The University of Worcester will continue to monitor the use of the equipment and revisit the Privacy Issues and Risks through ongoing consultation with the University and local community, together with responding to any national and legislative changes.

Purpose of Data Protection Impact Assessment (DPIA)

Any project or set of new processes that involve exchanging personal information has the potential to give rise to privacy concerns, from the public. This document is a method by which to alleviate any public concerns for the use of this relatively new technology.

What is meant by privacy?

Privacy, in its broadest sense, is about the right of an individual to be left alone. It can take two main forms, and these can be subject to different types of intrusion:

- Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of

communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

The Data Protection Impact Assessment is a process which helps organisations to anticipate and address the likely privacy impacts of projects, in order that problems can be foreseen and solutions developed to ensure that concerns are addressed appropriately.
The University of Worcester, has introduced the use of body worn cameras that are capable of capturing both moving images and audio information, which are worn by uniformed security staff. The aim of undertaking this PIA is to explain the extent of

- Their use
- Their limitations
- How any data captured will be processed
- An analysis of the rights to privacy of citizens and the risks that this could impose on it's the introduction.

This DPIA only addresses the application of this equipment in an overt capacity.

What is Body Worn Video (BWV)?
Any style of camera, which is carried or fixed to the uniform of a security officer and is capable of capturing both video and audio information collectively falls under the category of Body Worn Video.

The equipment used is supplied by CEESC has been in use by police forces and in other public facing roles for a number of years, with advancing technology the devices have become smaller, lighter, more easily carried by staff and have far greater capabilities in when and where they can be used. In addition, the actual quality of the captured data is now of a high standard. The devices themselves are generally mounted on an officer's uniform.

The BWV has been designed with law enforcement in mind - users cannot delete or overwrite footage on the camera and the encryption makes all footage completely unreadable except by authorised computers. A tamper proof digital fingerprint and encrypted memory securely keeps track of every file, completing the evidential trail from capture to production of a DVD. Images are high resolution providing evidential quality images suitable for criminal proceedings.

Why use BWV?
The University of Worcester has a responsibility to maintain the security and safety of staff and students and those other persons who visit University property. This will involve security staff stopping and speaking to people and recording information. In some instances, the rigour of what has been recorded has been the subject of interpretation and the subject of debate. Equally it may not have presented the best possible primary evidence to support a prosecution.

By the introduction of this type of technology, the devices themselves are able to record exactly what happened, what was said and when, in an indisputable format. Their use will be at the discretion of an officer and should:

- Meet a pressing need
- Incident specific
- Proportionate
- Legitimate

- Necessary and Justifiable.

BWV must be seen as being complementary to the University's CCTV system and other methods that security staff already use to record information.
This equipment may therefore be used to record video and audio information of encounters between the security staff and the public, after ensuring appropriate safeguards in respect of the necessity, legitimacy and legality and that in pursuance of the University's CCTV codes of practice.

- Assist in providing a safe and secure environment.
- Reduce crime and the fear of crime by reassuring students, staff and visitors.
- Deter and detect crime, public disorder and anti-social behaviour.
- Identify, apprehend and prosecute offenders in relation to crime, public disorder and antisocial behaviour.
- Provide the Police, Health and Safety Executive and University with evidence upon which to take criminal, civil and disciplinary action respectively.
- Protect security staff from undue threats and violence.
- Obtain evidence for use in the investigation of criminal actions, breaches of health and safety legislation and breaches of student and staff disciplinary procedures

In addition, persons, unrelated to any specific interaction or incident might find themselves captured on a BWV device. To some degree, this is inevitable since a camera lens or microphone is nondiscriminatory and captures what is seen or heard. In such circumstances, the University of Worcester has adopted a number of safeguards to firstly avoid this where possible and to then anonymise any data.

As previously mentioned, BWV is capable of capturing primary evidence in such a way that it is able to bring a compelling and an indisputable account of the circumstances at that time. This will not replace the needs to capture other types of evidence but will go a considerable way in reducing any ambiguities and should be considered as an additional security aid.

BWV will not be routinely recording and monitoring all activity on a continuous basis. To do so would fundamentally breach the privacy of large swathes of the public, who are going about their legitimate lives, as well as the privacy of staff going about their work. This cannot be justifiable from the perspective of proportionality and legitimacy.

Added to this, is that current technology is incapable of operating in such a way principally due to a lack of suitable battery life. In addition, such a practice would require the storing, reviewing and then disposal of large quantities of data.
The equipment will be worn by uniformed security staff and the use will be primarily driven by the incidents and circumstances presented to them or in anticipation of responding to a reported and unfolding incident.

A BWV downloads to windows media player and is used to maintain the integrity and continuity of the device and captured BWV video evidence. A procedure has been issued on the correct use of BWV and downloading of information.

During the course of their normal patrol, the device remains in an inert state and therefore is not recording any material. In order to do so, it requires the officer to deliberately activate the device to a record mode and where practicable, make a verbal announcement to indicate that the BWV

equipment has been activated. This announcement should be present on the recording and if possible, should include:

- The date, time and location;
- The nature of the incident to which the user is deployed; and
- Confirmation to those present that the incident is now being recorded using both video and audio.

If the recording has commenced prior to their arrival at the scene of an incident the officer should, as soon as is practicable, announce to those persons present that recording is taking place and that their actions and sounds are being recorded. Announcements should be made using straightforward language that can be easily understood by those present. At the conclusion of any incident, the record mode on the device is switched off and the captured information is stored.

Unless specific circumstances dictate otherwise, recording must continue uninterrupted from the moment it starts until the conclusion of the incident or the resumption of general patrolling.

The recording is also likely to continue for a short period after the incident to clearly demonstrate to any subsequent viewer that the incident has concluded and that the user has resumed other duties or activities.

Where practicable, users should make an announcement that the recording is about to finish. Prior to concluding recording, the user should make a verbal announcement to indicate the reason for ending the recording. This should state:

- The date, time and location;
- The reason for concluding the recording.

At the end of the period of duty, the officer returns the BWV to the Control Room and following a clearly defined process which, in effect involves the officer 'checking in' the device into the control room where it will be downloaded to the control room PC. This information cannot be deleted or altered. The officer will then identify the elements of any captured data that is to be retained to assist in an investigation, and 'mark' the section appropriately, by using the built in software.

Once completed, the contents on the BWV are erased and it is ready for reuse. All information captured and downloaded will be retained on a computer. Any material required to support an ongoing investigation or prosecution will be retained as fulfilling a 'lawful purpose'

All other material will be automatically erased after 9 days. Access to recordings will be controlled and only persons having an operational need to view specific incidents may do so. All video captured will be managed in accordance with relevant legislation and the University's CCTV code of practice.

Identified roles

In line with the University of Worcester's CCTV code of practice the following roles have been identified for the management of the BWV system.

Data Controller - University of Worcester
Data Manager – Assistant Director – Security & Operations

Data Administrator -

The University's use of BWV is determined to be lawful (under common law,) proportionate, necessary, justifiable, addresses a pressing social need and that the evidence it provides cannot be achieved through less intrusive means.

Surveillance Camera Commissioner's 12 guiding principles

The University of Worcester complies with the Commissioner's principles as recorded below:-

1 What's your system for
Do you review its use?

2 Have you carried out a privacy impact assessment?
Do you publish your privacy impact assessment?

3 Do you have signage in place to say surveillance is taking place?
Is there a published point of contact for people to raise queries or complaints with?

4 Who's responsible for your system?
Are your staff aware of their responsibilities?

5 Do you have clear policies and procedures in place?
Do your staff know what your policies and procedures are?

6 How long do you keep images/information?
How do you make sure images/information is deleted once they're no longer needed?

7 Do you have a policy on who has access to the stored information?
Do you have a policy on disclosure of information?

8 Do you follow any recognised operational or technical standards?

9 Do you make sure that the images captured by your system are caught securely?
Are only authorised people given access to the images?

10 Do you evaluate your system regularly to make sure it's still required?
Could there be an alternative solution to a surveillance camera system?

11 Can the criminal justice system use the images and information produced by your Surveillance camera system?
Do you have a policy on data storage, security and deletion?

12 Do you use any specialist technology such as ANPR, facial recognition, Body Worn Video (BWV) or remotely operated vehicles (Drones)?
Do you have a policy in place to ensure that the information contained on your database is accurate and up to date?

European Convention of Human Rights Act 1998

The use of BWV is viewed as an interference of Article 8 'The right to respect for private and family life, home and correspondence' and Article 6 'The right to a fair trial' These are qualified rights and the University has put in place suitable safeguards, including written procedures, staff training and secure IT systems.

Expectation of Privacy

Individuals are likely to have a strong expectation of privacy, in places not generally open to the public, such as a private residence especially at a time of day when people are likely to be in bed. Clear justification of the necessity to use BWV will be required in such circumstances. Furthermore circumstances may dictate an expectation of privacy, even when an incident has occurred in a public area, such as where someone may be the subject of an accident in the street.

Likely to cause serious offence

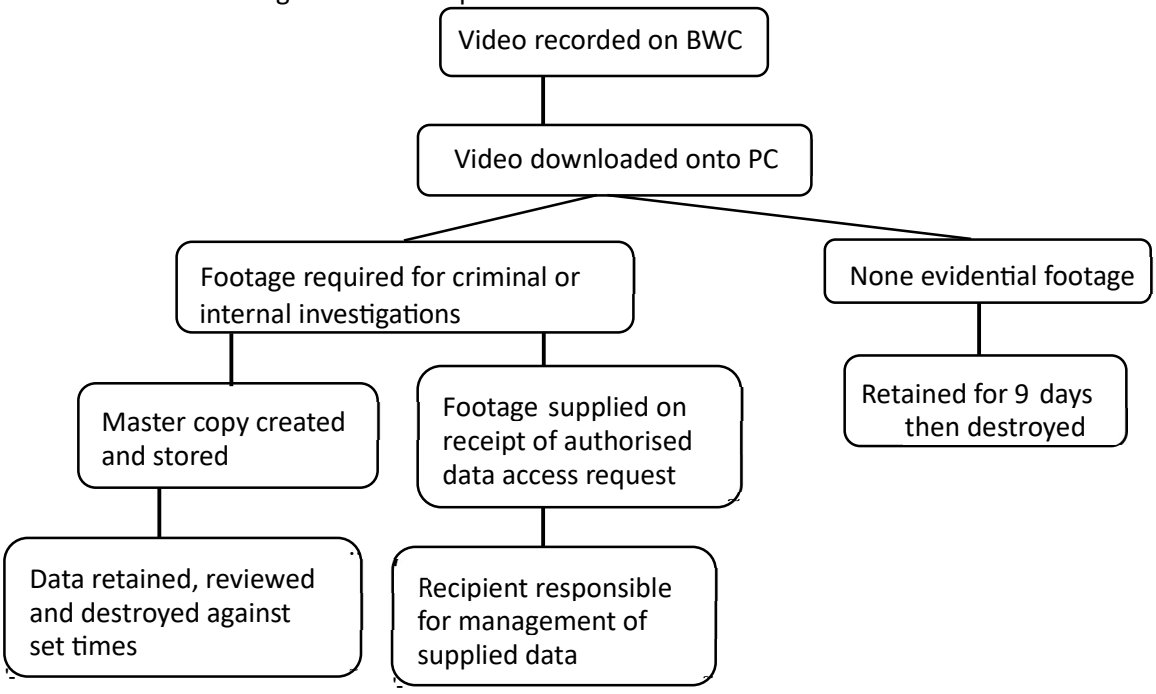
Care should be exercised in using BWV where it may cause serious offence, for example during a religious ceremony.

Data Flow

The chart below demonstrates how information captured on a BWV device is processed and then disposed of. The University of Worcester has the responsibility for the processing of information in its possession which commences at the point when capture by a Security Officer.
Clearly, when information is identified as being non-evidential, this follows a process whereby it is automatically deleted after 9 days.

In circumstances where the information is evidential, master copies are created and retained. At the conclusion of any investigation, there is a requirement to hold the data strictly in accordance with the Data Protection Act requirements, which includes undertaking appropriate reviews, further retentions if appropriate and then disposal.

Where information is passed to law enforcement agencies, those agencies take on the responsibility for the retention management and disposal of that information.



Privacy Issues and Mitigations

Through the introduction of this type of technology, there might naturally be concerns associated with how any information is being captured, processed and retained by the University of Worcester. The purpose of this section is to firstly identify what these issues are and to then provide an explanation of the mitigation the University of Worcester will apply, to ensure the risks are kept to a minimum.

BWV introduces new and additional information technologies that have a substantial potential for privacy intrusion
BWV is an expanding technology being utilised by the University of Worcester. The public's concerns with regard to privacy issues are recognised. Accordingly, this technology will only be deployed in an overt manner, using trained uniformed staff and in defined operational circumstances. All captured data will be processed to ensure compliance with the Data Protection Act and Human Rights Act 1998, Information Commissioners Code of Practice and Surveillance Camera Commissioners guidance.

BWV technology allows information to be shared with multiple agencies?
When capturing information on these devices, staff will only do so in order to fulfil a lawful purpose. The legitimate purpose behind the use of this equipment is to prevent and detect crime and prevent public disorder. When information is captured, it will firstly be assessed as to whether it constitutes evidential or non-evidential material. Any material, which is deemed as evidential, could then be shared with the Police and other prosecuting agencies and to managers undertaking internal investigations. There are occasions when BWV material could be shared with other agencies to assist in training and to support a multi-agency approach to any legitimate, justified working arrangement. The BWV and the software used supplies data in a format suitable for sharing with those agencies that may request the data.

How will any information be shared with those Agencies that may lawfully require the video evidence
Any captured information deemed to be evidential, will be provided to the investigating organisation pursuant to the systems objectives. Both a sealed master and a working copy will be created and passed to the requesting organisation. The images on the system will be archived until such time as the investigation is resolved at which point they will be permanently erased.

Is the data processing exempt from legislative privacy protections?
The University of Worcester will only deploy this technology against the defined operational requirements and to ensure that the use is proportionate, legitimate, necessary and justifiable. In addition, it will ensure that the use satisfies the requirement of addressing a pressing social need. At all stages it will comply with the Data Protection Act and other legislation. In the case of the Human Rights Act 1998, there will be adherence to the requirements of Article 6 (Right to a fair trial) and in respect of Article 8 (Right to respect for private and family life, home and correspondence) since this is a qualified right, information will only be captured and processed to achieve a legitimate aim as detailed earlier.

Will the handling of any data change significantly to be of concern?
The University currently capture digital evidence from CCTV systems and process this in accordance with legislation and strict codes. The University are accredited with the Home Office and have the Certificate of Compliance. BWV provides another source of information, but there are a number of significant differences. Firstly this technology allows the capture of both video and audio data which differs from CCTV but a principle issue is that without the introduction and adherence to essential safeguards, there is the greater risk of the possibility of widespread intrusions into the privacy of citizens. However there are appropriate policies and legislative requirement imposed on its use, and The University of Worcester is confident that these will minimise this risk.

Will BWV significantly increase the quantity of data captured and processed in respect of that held on any one individual or a wider group?
BWV is a relatively new technology and is seen to have major benefits of capturing evidence in an indisputable fashion. Accordingly, there will be more data potentially being captured but the appropriate safeguards, by adherence to legislation and guidance, will ensure that only information that passes a strict test, of being required for a lawful purpose, can be retained.

What are the safeguards for minimising the retention times for data?
Any information captured on a device, which is deemed to be non-evidential will be automatically deleted after a set period of time (9 days). The rationale for any retention beyond an immediate disposal might include circumstances where there is a desire to review any allegations as part of the University's complaint procedure, the reporting of these more often occurring the aftermath of any incident and often this material may not have been marked as evidential. Other data within the evidential category will be retained in order to satisfy the requirements of legislation, the court process if applicable and depending on the type of offence retained, reviewed and disposed of, in accordance with timeframes within the Data Protection Act, currently the University of Worcester retains all CCTV evidential material for a maximum of 9 days.

What are the procedures for dealing with the loss of any BWV devices?
Users are instructed that BWVs' should be held securely when not being worn. BWVs' when not in use will be placed in the Control Room, located within the access controlled area. Due to the nature of Security patrolling, it is possible such as within a public order or violent encounter that a device might be lost and fall into the hands of unauthorised persons. Where a device is lost, all possible attempts will be made to identify and notify persons who are subject of information on the device. The University of Worcester will also notify the Surveillance Camera Commissioner's Office at the earliest opportunity. In response the following safeguards have been put in place;- • The University of Worcester adopts a process whereby the devices are booked in and out at the start and end of an officer's duty. Accordingly, the impact in terms of any time lost between any actual loss and notification to the University, is kept to a minimum. • The data held on the device is protected and data cannot be accessed from the device itself. • Data is downloaded onto the desktop, and then deleted from the device. The system is encrypted and can only be accessed by authorised persons using their username and password.

Access to stored data is restricted and dependent on an individual's role.

Audio Recording is a greater infringement of my privacy, how can this be justified?

BWV is seen to have major benefits of capturing evidence in an indisputable fashion. In order to ensure that all aspects of an incident are captured, this requires the essential inclusion of audio information in order for this to be complementary to the video data. The other important aspect of the addition of audio information is that in some instances, the camera itself may not be pointing in the direction of the main incident but that the audio will still be captured. This has a significant advantage of protecting all parties to ensure that the actions of security staff were totally in accordance with the law and addresses issues of transparency. Equally, in some instances, the presence of only video evidence without the added context that audio, can fail to adequately provide the full context, for all parties, of an incident or interaction.

Collateral intrusion is a significant risk, how will this be handled?

Collateral intrusion in this context extends to the capturing of the movements and actions of other persons when this equipment is being used. It is inevitable that in some circumstances this will occur, albeit staff are trained to ensure that wherever possible, the focus of their activity is on the person subject of the officer's attention.
In circumstances where unrelated persons are captured in any video or audio information their identities will be protected and anonymised especially should the matter be presented in proceedings.

Do you need consent to record an individual?

It is important to note that there is no requirement to obtain the consent of the person or persons being filmed since the actions of the user are deemed to be lawful. In the event that someone requests that the BWV be switched off, the security officer should advise the person that:

- Any non-evidential material is only retained for a maximum of 9 days
- This material is restricted and cannot be disclosed to third parties without the express authority of the subject of the recording unless prescribed by law; and
- Recorded material is the University of Worcester's information and that it can be accessed on request in writing in accordance with the DPA 1998, unless an exemption applies in the circumstances. Data Protection Act 1998.

The BWV operator will consider on a case-by-case basis whether or not to switch the BWV off. There should always be a presumption to record if the 'need to address a pressing social need' has been achieved unless the circumstances dictate otherwise. An officer failing to record an incident may be required to justify the actions as vigorously as any officer who chooses to record a like encounter. In all cases, recording can only be justified when it is relevant to the incident and necessary in order to gather evidence.

Are you allowed to record in private dwellings?

It is widely recognised that citizens are likely to have a strong expectation of privacy especially in their own homes. Indeed this is contained with Article 8 of the ECHR (a right to respect for a private and family life) and under normal circumstances BWV should not be used in private dwellings. However if a security officer is present at an incident in a private dwelling and is there for a 'genuine lawful purpose' and this equipment is able to address a 'pressing social need' then the security officer can consider making a BWV recording in the same way in which any other incident is recorded.

The security officer will be mindful to exercise discretion and recording should only be used when it is relevant to the incident and necessary in order to gather evidence, where other reasonable means of doing so are not available. All recordings require a lawful basis in order to justify infringement of Article 8.

In circumstances where an occupant of the premises objects to the recording taking place but where an incident is taking place or allegations of a criminal nature are being made, security staff are recommended to continue with a recording but explain their reasons for doing so.

These reasons might include:

- That an incident has occurred requiring a security staff to attend
- That the security officer's continued presence might be required to prevent a breach of the peace or injury to any person
- There is a requirement to secure best evidence of any offences that have occurred and that the video/audio evidence will be more accurate and of a higher quality and therefore in the interests of all parties
- That continuing to record would safeguard both parties, with a true and accurate recording of any significant statement made by either party and of the scene.
- That the incident may reoccur in the immediate future or that continuing to record will safeguard the BWV user against any potential allegations from either party.

The University of Worcester is very mindful of the concerns that this raises and has trained its users to respect and adhere to these safeguards.

Item	Name	Date
Author:	Tom Taylor	
Approved by:	VCEB	30/07/2026
Version :	1.2	