DOCUMENT CONTROL INFORMATION				
Date	Version	Status	Editor	Comment
03/08/2017	BWV 02 V1	Expired	CN	
26/8/2017	BWV 02 V2	Expired	CN	
036/8/2018	BWV 02 V3	Live	CN	Annual Review

EBORACUM

Role/Site/Client **N/A.**

Name of Policy/SOP:	**Body Worn CCTV Privacy Impact Assessment**
References:	Data Protection Act Surveillance Camera Commissioner's code of practice Information commissioner's office code of practice Human Rights Act Client Requirements / Specification S24a Police and Criminal Evidence Act S5 Serious Organised Crime and Police Act BWV01 -Body Worn CCTV Policy & Procedures.

SOP Brief/ Introduction

Introduction and Screening Questions

It is widely known that citizens, going about their daily lives, are likely to have their movements and identity captured on surveillance systems. Therefore, it is important to mitigate any privacy risks and issues. This Privacy Impact Assessment has been written to explore these issues and in particular to explain:

- The rationale for Eboracum UK using this technology
- The legality behind its use
- The likely operational circumstances where operatives may use BWV
- Key privacy issues and risks and an explanation on their mitigation

The company deploy Body Worn CCTV with operatives inline with BWV01 Body worn CCTV Policy and Procedures.

SOP Details:

The Information Commissioner's Office Code of Practice recommends the application of 'screening questions' to confirm or otherwise the requirement for a Privacy Impact Assessment and to indicate its appropriate scale and detail. These questions are re-produced in the table below:

No.	Question	Response
1	Does the project apply new or additional information technologies that have the potential to invade the privacy of any individuals and/ or employees?	Yes. BWV (although overt) is proximate to incidents and events and therefore has the potential to invade the privacy of individuals, as well as the officers carrying them.

2	Does the project hold sensitive information that could potentially expose the identity of the individuals and/ or employees and require new security measures	Yes. BWV holds personal data requiring secure environment for storage and use of data.
3	Does the project have the capacity to continue without identifying any of the individuals and/ or employees?	No. Only identified employees have access to the BWV camera software. No unidentified employee has access to this software.
4	Does the project involve working with multiple organisations, whether they are government agencies or private sector organisations (e.g. as outsourced service providers or as 'business partners')?	Yes. Due to the nature of the specified purposes, there is likely to be sharing of data with North Yorkshire Policy, the City Of York Council and other third parties/private sector organisations.
5	Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals and/ or employees?	Yes. Images of people whether victims, suspected offenders, witnesses, bystanders, employees or Police officers will be captured on BWV before secure but accessible storage.
6	Does the project involve new or significantly changed handling of a considerable amount of personal data about each individuals and/ or employees in the database requiring new retention arrangements?	Yes. The uploading and storage of images is the core of the BWV system.
7	Does the project involve new or significantly changed handling of personal data about a large number of individuals and/ or employees?	Yes. The actual length (amount) of footage and what proportion is categorised as evidential and therefore retained, will be closely monitored at executive level.
8	Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?	No. Although as a caveat, providing evidence to build prosecution cases could involve the creation of composite video evidence e.g. bringing together BWV and CCTV however this would be carried out by appropriate authorities.
9	Does the project relate to data processing which is in any way exempt from legislative privacy protections e.g. The Data Protection Act?	The company is not a public sector organisation and is **NOT** exempt from any legislative privacy protections such as national security etc.
10	Does the project's justification include significant contributions to public security measures?	Yes. Included in the social need of the prevention and detection of crime, is public safety and security.
11	Does the project involve disclosure of personal data to, or access by, third parties that are not subject to similar privacy impact audits?	Yes. Disclosure will be to other public bodies; police services, the Courts and NHS Trusts.

12	Will the project be subject of consultation both internally and externally	Yes. The scheme is audited and internally reviewed annually. It will be externally audited buy a Third Party approved by the Surveillance Camera Commissioner.

What is a Privacy Impact Assessment and what is the need for it?

Any project or set of new processes that involve exchanging personal information, inevitably gives rise to privacy concerns from the public. The data collection, sharing and processing must therefore be undertaken within a clear legal framework with minimum intrusion on an individual's privacy.

A Privacy Impact Assessment (PIA) can assess privacy risks to individuals as part of the collection, use and disclosure of information, within projects and policies that involve the processing of personal data. It enables the company to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved. This PIA only addresses the application of BWV equipment in an overt capacity.

Street rangers, Security Staff and Taxi Marshals, in going about their daily routine, may suffer abuse and a significant threat to their personal security/safety, be this via physical or verbal means. Members of the public may witness such abuse or may themselves be subject to it. Likewise, in going about their daily routine, our staff routinely suffer verbal abuse and can be subject to complaints from the public due to the nature of the role they perform. Often in all these situations factual evidence of what took place is confined to one person's word against another. This does not leave the company in a satisfactory position and the safety of our people is indisputably put at risk.

The company has invested significantly in procuring Body Worn CCTV, managing the processes and arranging external auditing. Any project or set of new processes that involve exchanging personal information, inevitably gives rise to privacy concerns, from the public. Indeed, the cumulative effect of many such initiatives during recent decades has resulted in harm to public trust and to the reputations of corporations and government agencies alike.

The PIA will ensure that individuals and wider communities have confidence that BWV devices are deployed to protect and support them, rather than spy on them.

This PIA has been written to explore these issues and in particular to explain:

- **The rationale for Eboracum UK Ltd using this technology.**
- **The legality behind its use.**
- **The likely operational circumstances when employees may use it.**
- **The key privacy issues and risks and provides an explanation as to how the organisation mitigates them.**
- **How Eboracum UK will continue to monitor the use of the equipment .**

The Information Flows

Eboracum UK has the responsibility for the processing of information in its possession which commences at the point when an officer captures it. The internal procedures given to all staff who use BWV devices, demonstrates in simple terms, how information captured on a BWV device is captured, processed and then disposed of.

The general privacy and related risks of surveillance technology.

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 an organisation.

So far as surveillance and data storage is concerned the general risks are:

1. Inappropriate collecting of images.
2. Retention period of images too long or not long enough.
3. Risk of disclosure in normal usage (e.g. monitors and images viewable by the public).
4. Risk of accidental disclosure (poor procedures and inadequate training of staff processing the data).
5. Risks associated with intentional or legally required disclosure, e.g. S7 subject access requests**.**

The privacy and related risks of BWV

Privacy Issue	Risk to Individuals	Compliance Risk	Eboracum UK Corporate Risk
Collection of data	Contravention of privacy rights Unauthorised access to data	Data Protection Act 1998 - contravenes Principle 1 (fair and lawful processing)	The Data Protection Act comprises eight principles and data controllers have a legal obligation to comply with these principles. The data subject must be informed of: the identity of the data controller; the purpose or purposes for which the material is intended to be processed; and any further information that is necessary for processing to be fair. The data controller is the Managing Director of Eboracum UK Ltd. Data losses which damage individuals could lead to claims for compensation. The data will be stored in secure environment at Eboracum UK offices with access granted only to employees who have had specific training, permitted on authority of the Managing Director. BWV cameras will not record at all times (they can be turned on and off) and will be automatically deleted after 28 days.
Loss or misuse data	A failure to account for a full audit trail Footage being kept for longer than necessary	Data Protection Act 1998 - contravenes Principle 7 (security)	
Footage being recorded unnecessarily	If a retention period is not established information might be used for longer than necessary.	Data Protection Act 1998 - contravenes Principle 3 (excessive)	

Recorded images (in private property as opposed to public Areas.	Potential Misuse of footage	Human Rights Act 1998 – contravenes Article 8 (the right to respect for private and family life, home and correspondence)	The use of BWV must be shown to be proportionate, legitimate, necessary and justifiable. In addition, use of the equipment should address a 'pressing social need' especially in respect of its application within the confines of the Articles enshrined by the European Convention of Human Rights (incorporated into the Human Rights Act 1998). In relation to private property – unless assumed contract-related filming takes place, permission will be sought verbally prior to recording. The body cams are not used in private dwellings. Public distrust about how information is used can damage an organisation's reputation. In respect of the Human Rights Act, Eboracum UK is satisfied that the use of BWV is necessary, legitimate and proportionate. Note: Eboracum UK ltd cannot technically breach article 8 due to not being a public body therefore.
The use of images in court proceedings	Measures taken against individuals as a result of collecting information about them might be seen as intrusive	Human Rights Act 1998 – contravenes Article 6 (the right to a fair trial)	
The use of images in court proceedings	The information provided may be beneficial to the prosecution or the defence	Criminal Procedure and Investigations Act 1996	Any images to be used in court are seized, handed to relevant authorities to process for that purpose. Eboracum have no control of the use of data in that respect. An audit trail of footage provided to Police/Other authorities will be maintained.

The potential for covert surveillance	Contravention of privacy rights	Regulation of Investigatory Powers Act (RIPA) 2000	RIPA Does not apply to Eboracum UK due to it not being a public sector body or organisation. The use of BWV is intended to be overt however the devices may be deployed for covert filming for gathering of evidence under specific instruction from a client on their own premises. In relation to public places- there is no law against filming in public places with the exception of terrorism related legislation. Operatives will announce the use of BWV on all occasions where practical. (Defined in BWV01).

Solutions to the Privacy Risks

Risk	Solution
Collection/ use / loss of data	Access to data only available to management with a valid SIA CCTV License and director approved staff within the company. Persons entitled to access data identified in CCTV Code of Practice. All data signed for by person receiving the data. For full disclosure, publish the PIA and Policy & Guideline documents on the public website.
Footage being recorded unnecessarily	The process has been properly set up to retain data for the correct retention period (maximum 28 days, before deletion). This is with the exception of retained footage requested by Police where the data is stored for as long as the case is live, or in other circumstances where retention is applicable.
Recorded images (in private as opposed to public areas)	There will be a log of the booked out cameras, which shows the user who booked out the camera. Footage will NOT be permitted to be receded in private dwellings.
The use of images in court proceedings	All officers will receive training in all the necessary technical aspects of the equipment being used. This will cover the legal implications, equipment, practical use e.g. when to commence and cease recording, and health and safety.
The potential for covert surveillance	BWV will be deployed in an overt and covert manner using the same protocol on both types.

Evaluation of the Solutions to the Privacy Risks

Eboracum UK recognises the concerns from the public and customers regarding privacy issues. Accordingly, this technology will be deployed in an overt manner, using trained staff and in defined operational circumstances. Footage/images can only be reviewed by CCTV (SIA) licensed management. The use of BWV, both image and audio, has been investigated to ensure legislative compliance. All captured data will be processed and managed in compliance with the relevant legislation such as Data Protection Act, Human Rights Act 1998. It is important that a surveillance system produces information that is of a suitable quality to meet the purpose for which it was installed.

BWV systems are likely to be more intrusive than the more 'normal' CCTV style surveillance systems because of its mobility; however BWV also has the potential for positive outcomes for both the company, its customers , local partners and the public. It can, for example, help reduce the occurrence of intimidation and threat of violence.

The extension of BWV cameras only be used in accordance with the law and the specific privacy related impacts have been identified but are mitigated as set out below. The default retention period for BWV is 28 days and the system is audited.

Cameras are encrypted and can only be linked to a PC once a PIN number is presented.

Data collected from BWV cameras is not accessible to any other parties other than other authorised staff members. Once the data is downloaded from the device, it will be kept securely on a password protected PC. The PC is standalone with no connectivity to a network. It is kept in a secure office will be locked down to certain nominated users to ensure its safeguarding. Only nominated staff will be able to access the footage to view or delete recordings.

Misuse of the data constitutes serious misconduct and will be robustly dealt with should it ever happen. Auditing systems are in place to deter any such wrong doing and to identify it, should it happen.

Likely outcomes if these risks are not adequately addressed include complaints, drain on resources, damage to reputation and enforcement action and sanctions by ICO.

Review of the Privacy Impact Assessment

The system used will be regularly tested to ensure its efficiency in protecting the footage captured. Procedures will be regularly checked to ensure best practices are followed, to identify problems in the procedures and to amend / update them as necessary.

Eboracum UK Ltd will review the impact of BWV cameras from time to time.

This policy will be reviewed periodically and where a appropriate change is to be implemented/announced.

Approved By:	
Carl Nickson Director Date as per Ver Control.