

Swindon Borough Council
Body Worn Video Devices
April 2017

Privacy Impact Assessment

Contents

1. Introduction
2. Responsible Person Contact Details
3. Data Storage & Control
4. Camera Specific
5. Camera Specific –Post Installation Review Only

INTENTIONALLY BLANK

1. INTRODUCTION

Delivering services effectively requires Swindon Borough Council (SBC) to collect and hold large volumes of sensitive, personal and organisational information. This process has a number of risks including security, data quality and privacy. The council has a responsibility to ensure that its activities maintain appropriate security, privacy and quality controls and standards for its staff, customers, service users and other stakeholders.

A **PIA** considers the impact that the proposed project or activities will have on the individuals involved.

The four areas which are highlighted by ICO as potential areas for loss of privacy in relation to personal data are:

- the privacy of personal information
- the privacy of the person
- the privacy of personal behaviour and
- the privacy of personal communications.

'Personal data' as defined by Section 1 of the Data Protection Act means data which relates to a living individual who can be identified:

- a) from those data, or
- b) from those data and other information which is in the possession of, or is likely to come into possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

When considering the installation of a Body Worn Video Device (BWVD) an Operational Requirement (OR) must be produced. The OR must be referred to as part of the installation and camera review process to ensure it meets and continues to be effective in addressing the purpose for which it was installed.

2. RESPONSIBLE PERSON CONTACT DETAILS

Below are the contact details of the person most qualified to respond to questions regarding this Privacy Impact Assessment.

Name: Anna Marzec

Title: Data Protection Officer

Email: amarzec@swindon.gov.uk

Telephone: 01793 463404

3. DATA STORAGE & CONTROL

3.1 Where are the real time images from the BWVD displayed?

- Viewing of real time images is not possible. BWVD must be docked& uploaded to be able to view footage.

3.2 Who has operational access and ability to move the BWVD?

- Enforcement Officers using the BWVD has the capability to move the device to capture the images they deem necessary at the time.

3.3 Where are the recorded images stored?

Web based storage

3.3.1 What measures are in place to control access to the area in which the recorded images are stored?

BWVD suite is electronically access controlled and only accessible to restricted users and guests. Authorized managers may also access recorded images but do so in secure staff environments.

3.4 How are the images recorded?

Digitally to BWVD, then uploaded to Web Based Servers.

3.5 Who has access to the recorded images?

Access is granted under the conditions being met for the Data Protection Act 1998 (DPA), in particular Chapter 29 section 35 Access to Data Request and Subject Access Request. Authorized Managers have access to the recorded images.

3.5.1 How is access gained to the recorded images?

Signing into the Security Room and reviewing data, they must then have a log on to the secure software where the images can be reviewed.

3.6 How long are the images retained?

Minimum 28 days.

3.7 How are the images deleted?

Digitally the images are erased as they continually record.

3.8 When data is downloaded or copied for release to a third party how is the information recorded?

Access to data forms require filling in, these are viewed, accepted or rejected and recorded. Other agency data requests are recorded on a separate access database.

3.9 What processes are in place to ensure that data protection responsibilities are understood by persons receiving the data?

Information to their rights under the DPA is available online.

4. CAMERA SPECIFIC

4.1 What type of camera is being considered or being used?

Edisix VB200 – Video Badge

4.2 Is audio recording an available feature of this camera?

Yes, the BWVD may capture private dialogue during the course of necessary use, these will be uploaded & securely stored for a minimum of 28 days, access to these recordings is strictly controlled and external access to them would only be granted under the conditions being met for the Data Protection Act 1998, in particular Chapter 29 section 35 Access to Data Request and Subject Access Request.

4.3 Does this camera have any other camera specific or software related features such as Automatic Number Plate Recognition, Facial Recognition, movement analysis?

No.

4.4 Does the BWVD have the capacity to record personal information as defined in 3.1

Staff using the BWVD will be our own Civil Enforcement Officers (CEO), the device will only be recording when they are faced with a threatening situation by a member of the public while carrying out their duties. Access to this information is strictly controlled and may only be accessed by meeting the requirements identified in 3.5 & 3.5.1. The Human Rights Act, DPA and RIPA prevents unauthorized directed surveillance.

4.5 Is there any chance of this footage being released in the public domain?

Only in the case of a media release where the identification of an individual is required to assist in the investigation of a crime.

4.6 Is there a Data Protection Act compliant sign clearly displayed in close proximity of the BWVD to make people aware that it is in operation.

Yes.

4.7 Does the BWVD see in to any part of any property where there is an expectation of privacy?

No, the BWVD doesn't specifically look into private property however whilst undertaking activities on and off street, a CEO may capture footage of a property where privacy is expected, this would be unknown as the operator cannot see what the Badge captures at the time, and footage captured would only be viewed if criteria above has been met. When not faced with threatening behaviour the badge is not switched on, this includes walking through pedestrianized areas, unless enforcement activity is required followed by threatening behaviour.

4.8 What measures have been taken to prevent observation of these areas?

CEO's using the badges are doing so for their own safety & integrity, the badges are positioned as such they capture the area directly in front of the CEO whilst faced with person/s who are showing signs of threatening, aggressive and verbal threats made towards the CEO. Staff should not actively capture footage of properties, properties may be in the vicinity given the nature of the environment and the work they undertake.

BWVD have been introduced as part of the CEO's personal protective equipment (PPE), one to one training is provided to each CEO prior to first use, which covers operation of the device and when and how the device should be used, each CEO confirms by signature to say they have received training and understood how to use and when the device should be used.

As BWVD are being used as CEO PPE, and when they take their annual conflict resolution refresher this will include refresher training being undertaken at the same time.

4.9 Does any additional action need to be taken to reduce the impact on privacy by the device?

Yes, BWVD refresher training, included as part of the CEO conflict resolution training.

5. CAMERA SPECIFIC – POST INSTALLATION REVIEW ONLY

5.1 Camera Number:

5.2 Has the purpose of the camera been reviewed?

5.3 Has the Council ever received a complaint relating to the impact on privacy by this device?

5.4 Give details of the source and nature of the complaint and the outcome.

Assessor

Signature: _____ Date: _____

Print Name: _____ Date: _____

Manager

Signature: _____ Date: _____

Print Name: _____ Date: _____

