

Staffordshire Police
Planning for Business Change
Information Systems and Technology

Small Scale Privacy Impact Assessment Report
Body Worn Video

Document Reference: **BWV PIA 0002 F**

Author: **Tricia Rich** **Date:** **11.11.13**

Change Control Record

Date	Document Reference	Change	By
11.11.13	BWV PIA 0001D	Creation of Preliminary PIA report	T Rich
9.5.14	BWV PAI 0002F	Finalise PIA report from feedback	T Rich

Contents

1. EXECUTIVE SUMMARY	3
2. INTRODUCTION.....	3
3. PROJECT BACKGROUND.....	3
4. LEGISLATIVE AND POLICY AUTHORITIES.....	4
5. DESCRIPTION OF PERSONAL INFORMATION.....	4
6. POTENTIAL PRIVACY AND DATA PROTECTION RISK	5
7. SECURITY REQUIREMENTS.....	6
8. RECOMMENDATIONS	7
APPENDIX 1.....	8

1. Executive Summary

The preliminary Privacy Impact Assessment indicates that the Body Worn Video should be the subject of this small scale PIA assessment.

2. Introduction

The Body Worn camera project is a replacement project for the existing ViewVu and RS2 cameras deployed across the county. There is in place a Force Policy on the use of Body Worn Video.

3. Project Background

The objectives of this project are:

- To increase officer safety
- To increase public safety
- To bring an increased level of successful prosecutions.
- To increase public confidence.

The existing cameras had ceased to function and project is aimed at delivering a force wide single product across Local Policing and Local Neighbourhood Officers, PCSOs and Special Officers. There will be 530 cameras across the county, and they will be deployed in stations that officers patrol from.

The project started in Proof of Concept (POC) in Newcastle LPT in July 2013, and the POC was signed off 30.10.13. Rollout will then continue across the other Local Policing Teams from November 2013-March 2014.

The project delivers new body worn cameras, new Digital Evidence Management system, and revised force policy on the use of Body Worn Video.

This project has indirect links into Mobile Data and Digital Interview recording and is part of the Mobile Data Project Board for governance purposes.

Stakeholders for this project include (but not exclusively)

- Operational policing
- Investigative services
- Justice Services
- CJS partners

Suppliers to this project include

- ICT
- Facilities
- Learning and Development
- Procurement and finance

The information being processed by this system is recorded video (and audio) footage, captured overtly by uniformed officers in the course of their duties in circumstances where they consider it is appropriate, lawful and proportionate, in accordance with the policy. The equipment is designed to give clear indication that it is recording.

The video footage may be used for evidential purposes:

- To establish facts or events to inform decisions about a prosecution or alternative out of court disposal
- As evidence in criminal courts or other judicial processes (eg Coroner's Court)
- In the case of an investigation into complaints against the police or misconduct matters.

The filming of members of the public and the retention of this information is subject to Police and Criminal Evidence Act (PACE), Criminal Investigations & Procedures Act (CIPA) and the Data Protection Act.

4. Legislative and Policy Authorities

The force policy on this, Body Worn Video – Use and Image processing, refers to:

Data Protection Act 1988 – fair processing
Police and Criminal Evidence Act 1984 (PACE)
Regulation of Investigatory Powers Act 2000 (RIPA)
Human Rights Act 1998
Freedom of Information Act 2012
Equalities Impact assessment
Management of Police Information guidance.
Article 8 of the Human Rights Act (HRA)

5. Description of Personal information

- Information processed
 - Video and audio recording of witnesses, suspects, and victims during the course of an incident
- Collection and use
 - Information is collected by the Body worn camera and stored locally on a SD card.
 - Data is recorded in high definition with sound
 - Once downloaded from the camera, the camera has the files automatically deleted
 - The files are then stored on a secure central server
 - Access to information on the server is controlled via Active Directory controls, and users must have been authorised by the LPT Commander to have access, after approved training has been given.

- As all data is stored on the central server, information is shared through the application DEMS on that server. No information is shared outside of the secure server, other than PAL DVD for Court, which is managed by CMU.
- Data can be stored as evidential (ie for use in a prosecution) or non-evidential. Non evidential data is automatically deleted after 31 days (DPA fair processing). Evidential data will be retained ad infinitum, subject to MOPI guidance on review. Any data subject to MOPI review will then be deleted manually by authorised personnel.
- Disclosure is via DEMS on police computers and is available in Interview rooms and Custody, as well as at CMU (for CPS review) . No discs or files are shared or transferred.
- For court purposes, evidence can be submitted via DVD, in PAL playback format.
- In due course, delivery of the video evidence to the CPS and Courts may be via a secure network connection
- Under the Criminal Procedure Rules, where a prosecution is pending, a copy of the recording may have to be released to the defence
- See appendix 1 for draft data flow.

6. Potential Privacy and Data Protection risk

- Members of the public are aware of the increased use of BWV through the national press and television news reports
- In Staffordshire, the PCC has been actively engaged in a public commination campaign at the start and end of the project, communicating the volume of cameras deployed, their usage and who will be using the cameras.
- Media queries on BWV are managed through the Office of the Police and Crime Commissioner and the Staffordshire Police Corporate communications department and all communication to the press and public is approved by them.
- Filming will involve members of the public and they may feel that their human rights are in some way breached by the filming. The Policy states the circumstances and permissions in law for filming, and this includes filming in private premises.
- Filming in private premises also poses a privacy risk, and is covered under PACE as well as under Data Protection Act – the policy makes clear the circumstances where filming is permitted and where it should cease.
- Stop and search is also another permitted use of body worn video, however under PACE filming must be stopped during a strip search.
- Collateral intrusion is also a privacy consideration, where people and events not relevant to the incident may be recorded. This may have to be subject to a technical redaction if footage is subsequently required in court.
- Members of the public have the right to issue a subject access request when they have been filmed. Such requests can be complied with, under

the current retention of records policy of 31 days for non-evidential recordings, and may have to be disclosed at any time if the footage has been marked as evidential.

- Viewing of footage is permitted at any Staffordshire Police station with a voluntary interview room. Viewing is also possible through the custody facilities
- Under the Freedom of Information Act, and FOI request is managed through our information security team and corporate communications.
- Viewing of data across the force is managed by the user account , and users are only granted access when it is a requirement of their role to view footage and appropriate training has been given

7. Security requirements

The following measures have been taken to protect personal data from unauthorised access, modification and disclosure

- Access and use
 - User access is approved by LPT Commander or Ch Insp equivalent.
 - Access is then granted by Technology services, once approval has been received
 - No users are authorised to view footage until they have had appropriate training on the DEMS system
 - Log in is managed by the active directory profile, which means users must log onto the computer with their user name and password
 - All access and use is monitored via collar number and every transaction can be subject to scrutiny by management or professional development
- Modification
 - The files in DEMS cannot be edited, nor can they be deleted by users.
 - Files cannot be modified or deleted on the Body Worn Camera
- Disclosure
 - All disclosure of unused materials is via the central server DEMS application. No data is shared outside of that, other than the video copy required by the court, which is handled by the Case Management Unit (CMU.)
 - Requests from foreign forces and other agencies are managed on an individual basis and the default is that other forces or agencies would first view the footage at one of the station facilities before any data is release.

Retention of records policy is :

- Non evidential files are deleted automatically by the system at 31 days
- Evidential data is held subject to MOPI guidance according to the offence involved and subject to regular review. Data that is identified as being subject to deletion under MOPI guidance is then deleted with Superintendent authorisation (Justice Services)

8. Further Recommendations

The system has a number of security features that significantly reduce the risk of disclosure of private data or amendment of said data.

The BWV project is a replacement project and was already subject to a Privacy Law and Data Protection Act compliance check as part of the policy review.

The nature of the material also indicates that under some circumstance data may need to be held more privately (to prevent inappropriate viewing), and this is one feature of the next software release

Appendix 1

Data flow for video and image handling

