EASTLEIGH BOROUGH COUNCIL

CORPORATE POLICY AND PROCEDURES

BODY WORN VIDEOS

Version 2 – August 2022

INDEX

APPENDICES

SECTION	APPENDIX
1	LEGAL SERVICES MANAGER
2	BWV AUTHORISED OFFICERS
3	DATA PROTECTION IMPACT ASSESSMENT TEMPLATE FOR SURVEILLANCE CAMERAS
4	BWV OFFICERS
5	BWV STAFF USER GUIDE
6	BWV THIRD PARTY DATA SHARING REGISTER
7	BWV SAR GUIDANCE CHECKLISTS
8	TRAINING REGISTER

INTRODUCTION & KEY MESSAGES

1. This policy sets out the statutory framework and procedures which permit the Council's lawful use of the overt surveillance technique known as Body Worn Videos (BWV).

2. The Human Rights Act 1998 (HRA) gave effect in UK law to the rights of individuals enshrined in the European Convention on Human Rights 1950 (ECHR). Some rights are absolute whilst others are qualified, thus is it permissible for the state to interfere with those rights, provided certain conditions are satisfied. One of those rights is a person's right to respect for their private and family life, home, and correspondence.[1] When public authorities seek to obtain private information about a person by means of overt surveillance, Article 8 is the most likely to be engaged, which may also give rise to issues under Article 6 (right to a fair trial).

3. This Corporate BWV Policy provides the statutory framework and the Council's guidance as to the use of overt surveillance camera systems, namely Body Worn Video devices, whilst ensuring the public authority does not infringe a person's Article 8 rights, except as may be permitted by Article 8(2). Consequently, a public authority can act in a way that is compatible with the ECHR and HRA.[2]

4. This Policy has been approved by the Cabinet[3] and in addition, the Audit & Resources Committee has an oversight role and carries out high level annual reviews of this Policy and processes.

5. Any member of staff who is unsure regarding any aspect of this Policy and/or the statutory framework, must contact the Council's Legal Services Manager[4] at the earliest opportunity. Compliance with this Policy and Process is mandatory for all relevant Council services and officers. This Policy is placed on the Council's Staff Hub.[5]

COUNCIL POLICY STATEMENT

6. Eastleigh Borough Council (EBC) takes its statutory responsibilities seriously and will always act in accordance with the statutory framework including relevant Orders, the Surveillance Camera Code of Practice, the Information Commissioner's Guidance on Video Surveillance[6] and Digital Imaging & Multimedia Procedure V3[7] Accordingly, the Legal Services Manager is duly authorised by the Council to monitor, review, and amend this Policy as and when

---

[1] ECHR Article 8
[2] Human Rights Acy 1998, Section 6
[3] 15 September 2022
[4] **Appendix 1**
[5] Insert link to Staff Hub BWV page
[6] Information Commissioner's Guidance on Video Surveillance 24/2/2022
https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/

[7] Published 16 November 2021
https://www.gov.uk/government/publications/digital-investigations-digital-imaging-and-multimedia-procedure/digital-imaging-and-multimedia-procedure-v30

required. For administration and operational effectiveness, BWV Authorising Officers[8] are authorised to add or substitute a BWV Officer [9] when required.

BODY WORN VIDEOS KEY BENEFITS & INTENDED USES

BENEFITS OF USING BODY WORN VIDEOS

7. BWV technology has a number of benefits and complies with specific objectives, including but not limited to:

- Significantly enhances the quality of evidence provided by law enforcement officers;
- Provides an independent, reliable, real time evidential capture of an event/incident as precisely as possible limited only by the field of view and audio range of the device;
- Promotes positive behaviour and interaction between the wearer and member(s) of the public;
- Assists in the drive to reduce crime and the fear of crime and increases the proportion of offences brought to justice
- Provides a greater impact than street CCTV as they can be deployed at any position within an incident; those present quickly learn the recordings include sound and BWVs are more obvious than other CCTV systems;
- Assists in the investigation of a complaint and/or alleged offence(s) arising out of an event/incident, thus reducing investigation time for unwarranted complaints;
- Assists the court to see and hear the incident through the eyes and ears of the officer at the scene, thereby gaining a real understanding of the actions of the accused;
- Time efficient saving by producing an exhibit of the recording, saving officer recording the incident as a statement or in their pocket notebook;
- Individuals prosecuted are more likely to plead guilty at any early stage when served clear recorded evidence of their actions, saving time and costs;
- Assists in officer development as there is an ability to review their performance in detail after an incident.

INTENDED USES OF BODY WORN VIDEOS

8. The use of BWV by Eastleigh Borough Council authorised officers is intended to assist in:

- Prevention and/or detection of crime and/or disorder;
- Criminal and/or civil proceedings arising out of the incident/event;
- De-escalation of a conflict/incident/event;
- Protection of staff who are acting in the course of their Council duties;
- Dispute resolution e.g., complaints against staff;
- Supporting the emergency services whilst undertaking their duties;
- Counter-Terrorism (Prevent Duty);
- Staff development training as to best practices;

BODY WORN VIDEO STATUTORY FRAMEWORK

[8] **Appendix 2**
[9] **Appendix 4**

9. The Protection of Freedoms Act 2012 governs the regulation of surveillance, specifically the Regulation of CCTV and other surveillance camera technology[10] and is supported by the mandatory requirement of a Surveillance Camera Code of Practice.[11]

SURVEILLANCE CAMERA CODE OF PRACTICE

10. Relevant authorities (including local authorities[12]) have a mandatory duty with regard to the Surveillance Camera Code of Practice (the Code), thus they must take the Codes into account when exercising any functions which consider the future deployment or continued deployment of overt surveillance. If a relevant authority decides to depart from the Code, they will have to have clear reasons for doing so.[13] The overarching purpose of the Code is to enable operators of surveillance camera systems to make legitimate use of available technology in a way that the public would right expect and to a standard that maintains public trust and confidence.

DEFINITION OF SURVEILLANCE

11. Surveillance for the purposes of RIPA 2000 includes [14]:

(a) monitoring, observing, or listening to persons, their movements, their conversations or their other activities or communications;
(b) recording anything monitored, observed, or listened to in the course of surveillance;
(c) surveillance by or with the assistance of a surveillance device.

12. Surveillance may be conducted with or without the assistance of a surveillance device, includes the recording of any information obtained and can be undertaken whilst on foot, mobile or static. Surveillance also includes references to the interception of a communication in the course of its transmission by means of a postal service of telecommunication system, if and only if [15]:

(a) the communication is one sent by or intended for a person who has consented to the interception of communications sent by or to them; and
(b) there is no interception warrant authorising the interception.

TYPES OF SURVEILLANCE

13. There are two types of surveillance, namely overt and covert.

OVERT SURVEILLANCE

14. Most surveillance carried out by the Council will be overt, thus it will fall outside the remit of RIPA. An example of overt surveillance is the Council's overt CCTV[16] and Body Worn Video devices.

---

[10] Protection of Freedoms Act 2012 Chapter 1, Sections 29-31
[11] Protection of Freedoms Act 2012 Section 29
[12] Protection of Freedoms Act 2021 Section 35(5)(a)
[13] R (on the application of London Oratory School Governors) v Schools Adjudicator [2015] & R (Munjaz v Mersey Care NHS Trust [2006]
[14] RIPA Section 48(2)(a)-(c)
[15] RIPA Section 48(4)
[16] https://www.eastleigh.gov.uk/media/2585/cctv-code-of-practice-2016.pdf

COVERT SURVEILLANCE

15. Surveillance is covert if and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.[17]

SURVEILLANCE CAMERA SYSTEMS

16. Methods of "recording" surveillance were expanded in Part 2 of the Protection of Freedoms Act 2012, which dealt with the regulation of CCTV and other surveillance camera technology and introduced the Surveillance Camera Code of Practice.[18] Surveillance Camera Systems include[19]:

(a) Closed circuit television (CCTV) or automated number plate recognition systems (ANPR);
(b) Any other systems for recording or viewing visual images for surveillance purposes;
(c) Any systems for storing, receiving, transmitting, processing, or checking the images or information obtained in (a) or (b);
(d) Any other systems associated with, or otherwise connected with (a), (b) or (c)

17. Body Worn Videos are captured within (b), as confirmed by the College of Policing Body Worn Guidance 2014 and AB v Hampshire Constabulary IPT/17/191/CH [2019][20]. Surveillance systems can be used to monitor and record the activities of individuals, often in high definition and with ease. These systems therefore capture information about identifiable individuals and how they behave which is likely to be personal data under data protection law. Accordingly, the Information Commissioner's Video Surveillance Guidance has been factored into this policy, as BWV is a scenario where personal data will be processed by a video surveillance system in the public sector.

SYSTEM OPERATOR

18. A person or persons that take a decision to deploy a surveillance camera system, and/or are responsible for defining its purpose, and/or are responsible for the control of the use or processing of images or other information obtained by virtue of such system.

SYSTEM USER

19. A person or persons who may be employed or contracted by the system operator who have access to live or recorded images or other information obtained by virtue of such system.

BODY WORN VIDEO

20. A body worn video (BWV) device is an overt portal system that provides an audio, video or photographic record of activities undertaken and/or witnessed by the wearer. This type of surveillance therefore has the potential to be more intrusive than conventional CCTV systems. Scenarios could include face to face on doorsteps and inside buildings such as homes and shops which increases the risk of privacy intrusion to individuals.

[17] RIPA Section 26(9)(a)
[18] First published June 2013, amended November 2021
[19] Protection of Freedoms Act 2012 Section 29(6)
[20] https://www.ipt-uk.com/docs/IPT%20Judgment%20-%20AB%20v%20Hants%20Constabulary.pdf

AUTHORISED OFFICERS

21. The Council has authorised the use of BWV by specific teams and their named BWV Officers[21], who are required to undergo training, before and in order to be authorised. The Council has also authorised specific officers to be given access to the BWV material, and to oversee the BWV Officers use of BWV, known as BWV Authorised Officers.[22]

PUBLIC PLACE

22. A public place is any highway and any place to which at the material time, the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission.[23] Please note, recordings of persons in public places are only public for those present so therefore still have the potential to be private. Recorded conversations between members of the public should always be considered private and consideration of a person's reasonable expectation of privacy is also relevant.

RELEVANT AUTHORITY

23. A relevant authority must have regard to the Surveillance Camera Code when exercising any functions to which the code relates.[24] For the purposes of fulfilling this statutory obligation, a relevant authority includes a local authority within the meaning of the Local Government Act 1972.[25]

FIRST MANDATORY TEST – IN PURSUIT OF A LEGITIMATE AIM

24. Examples of a legitimate aim and pressing need include:

- national security;
- public safety;
- economic well-being of the country;
- prevention or detection of crime and/or disorder;
- protection of health or morals;
- protection of rights and freedoms of others.

SECOND MANDATORY TEST – NECESSITY

25. Use of the surveillance camera system must be necessary for a pressing need(s). Any deployment should not continue for longer than necessary.

THIRD MANDATORY TEST – PROPORTIONATE

26. The purpose of the deployment must be proportionate to what is sought to be achieved. For example, is it proportionate to record both the visual and audio content of an incident? The technical design solution for such deployment should be proportionate to the stated purpose rather than driven by the availability of funding or technological innovation. The

[21] **Appendix 4**
[22] **Appendix 2**
[23] Public Order Act 1986 Section 16
[24] Protection of Freedoms Act 2012 Section 33(1)
[25] Protection of Freedoms Act 2012 Section 33(5)

decision as to the most appropriate technology should always consider the potential to meet the stated purposed without unnecessary interference with human rights.

SURVEILLANCE CAMERA CODE OF PRACTICE

27. The government is fully supportive of the use of overt surveillance camera systems in a public place whenever the use is in pursuit of a legitimate aim, is necessary to meet a pressing need, proportionate, effective, and compliant with any relevant legal obligations.

12 GUIDING PRINCIPLES

28. The starting point for a system operator in achieving the most appropriate balance between public protection and individual human rights, is to adopt a single set of guiding principles that are applicable to all surveillance camera systems in public places. The Code therefore sets out 12 guiding principles that should apply to all surveillance camera systems in public places:

1 SPECIFIED PURPOSE
2 EFFECT ON INDIVIDUALS & PRIVACY
3 TRANSPARENCY
4 CLEAR RESPONSIBILITY & ACCOUNTABILITY
5 CLEAR RULES, POLICIES & PROCEDURES
6 STORAGE
7 RESTRICTED ACCESS
8 STANDARDS
9 SECURITY MEASURES
10 REVIEW & AUDIT
11 USE IN MOST EFFECTIVE WAY
12 ACCURACY

29. Further assistance as to the 12 Guiding Principles is as follows:

1 SPECIFIED PURPOSE

30. Use of a surveillance camera system must always be for a **specified purpose** which is in **pursuit of a legitimate aim** and **necessary** to meet an **identified pressing need(s)**. The purpose(s) should be capable of translation into clearly articulated objectives against which the ongoing requirement for operation or use of the system(s) and any image(s) or other information obtained can be assessed.

31. To determine if objectives are met and identifying the appropriate technical solution, a system operator should always consider the requirements of the end user of the images, particularly where the objective can be characterised as the prevention, detection, and investigation of crime, where the end user is likely to be Legal Services Team and thereafter the criminal justice system. Once the specified purpose has been met, the BWV must be switched off.

2 EFFECT ON INDIVIDUALS & PRIVACY

32. The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular annual reviews to ensure its use remains justified. BWV is a

surveillance camera system; thus, consideration must first be given as to whether there is a less intrusive means than deploying the BWV. If not, the system operator must then consider if it is necessary and proportionate to capture both the visual and audio content of an incident.

3 TRANSPARENCY

33. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints. The Council has published a web page for the use of surveillance camera systems with specific reference to BWV and CCTV, which includes the Council's Corporate Complaints Procedure.[26] Transparency also requires informing the subject(s) you are capturing their personal data.

4 CLEAR RESPONSIBILITY & ACCOUNTABILITY

34. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held, and used.

5 CLEAR RULES, POLICIES & PROCEDURES

35. Clear rules, policies and procedures must be in place before a surveillance camera system is used and these must be communicated to all who need to comply with them.

6 STORAGE

36. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system and such images and information should be deleted once their purposes have been discharged.

7 RESTRICTED ACCESS

37. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8 STANDARDS

38. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9 SECURITY MEASURES

39. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10 REVIEW & AUDIT

[26] https://www.eastleigh.gov.uk/our-community/community-safety/cctv

40. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11 USE IN MOST EFFECTIVE WAY

41. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value**.**

12 ACCURACY

42. Any information used to support a surveillance camera system which compares against a reference database for matching purposes, should be accurate and kept up to date.

PROCESSING PERSONAL DATA BY VIDEO SURVEILLANCE SYSTEMS STAUTORY FRAMEWORK

43. Surveillance camera systems capture information about identifiable individuals and how they behave which is likely to be personal data under data protection law. The recently published Information Commissioner's Office Guidance on Video Surveillance[27] provides guidance for public authorities operating video surveillance systems that view or record individuals, including BWV. Information held by organisations that is classed as personal data relating to identifiable living individuals is covered by the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA). The seven UK GDPR principles for processing personal data are[28]:

i) Lawfulness, fairness, and transparency;
ii) Purpose limitation;
iii) Data minimisation;
iv) Accuracy;
v) Storage limitation;
vi) Integrity and confidentiality;
vii) Accountability

CONTROLLER

44. The Controller is responsible for and must be able to demonstrate compliance with the seven principles set out above. The Council exercises overall control of the personal data of identifiable individuals being processed, thus it is the "controller," of its surveillance system. EBC has therefore previously notified and paid the data protection fee[29] to the Information Commissioner's Office.

LAWFUL BASIS

[27] ICO Guidance on Video Surveillance 24/2/2022
https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/

[28] UK GDPR 2016 NO 679, Article 5 – Principles relating to processing of personal data
[29] Data Protection (Charges and Information) Regulations 2018

45. In order to process personal data obtained from the Council's surveillance systems at least one of the six lawful[30] bases must apply:

a) Consent;
b) Contract;
c) Legal obligation;
d) Vital interests;
e) Public task;
f) Legitimate interests;

46. It is likely the appropriate lawful basis will be legal obligation or reliance on a public task as BWV will be carried out as part of the Council's tasks as a public authority in the public interest.

SPECIAL CATEGORY & CRIMINAL CONVICTION DATA

47. Two further lawful bases for processing data are:

- Special Category Data — Require identification of Article 9 UK GDPR condition
- Criminal Conviction Data — Requires compliance with Article 10 UK GDPR

NECESSARY

48. Processing must be objectively necessary for the stated purpose. Many of the lawful bases for processing depend on the processing being necessary but it does not require processing to be absolutely essential. It must be more than just useful and standard practice.

PROPORTIONATE

49. Is the use of the surveillance system proportionate or is there a less privacy intrusive method of achieving the need where possible? If not, explain why these alternatives are not suitable or sustainable.

PERSONAL DATA

50. Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[31] Any recorded image and speech captured, which is aimed at identifying a particular person or learning about their activities, is personal data and so is governed by the Data Protection Act 2018.

SPECIAL (SENSITIVE) DATA

51. The UK GDPR defines special category data as:

[30] General Data Protection Regulation, Article 6(1)(a)-(f)
[31] General Data Protection Regulation, Article 4(1)

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**

52. This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply.

BIOMETRIC DATA

53. Biometric data means personal data resulting from special technical processing relating to the physical, physio-logical, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data.[32]

ACCOUNTABILITY

54. The accountability principle requires the Council to take responsibility of what it does with personal data, how it complies with the other principles and remains an obligation throughout the life of the processing. These principles include the requirements to[33]:

    - implement technical and organisational measures to ensure and demonstrate compliance with UK GDPR;
    - ensure the measures are risk-based and proportionate; and
    - review and update the measures as necessary

DATA PROTECTION BY DESIGN & DEFAULT

55. This concept requires the Council to consider data protection and privacy issues at the earliest stages of project planning.

PROCESSING RECORDS

56. The Council is required to maintain a record[34] of the processing activities taking place, which should include the purpose(s) of the lawful use of surveillance, any data sharing agreements, and the retention periods of any personal data.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

57. Prior to implementing this Policy, the Council has undertaken a Data Protection Impact Assessment to fully address its use of BWV which addressed any impact on the rights and

[32] General Data Protection Regulation, Article 4(14)
[33] General Data Protection Regulation, Article 24(1)
[34] General Data Protection Regulation, Article 30(1)

freedoms of individuals whose personal data is captured. Further, the Council will undertake a Data Protection Impact Assessment for any processing that is likely to result in a high risk to individuals. That includes:

- processing special category data;
- monitoring publicly accessible places on a large scale; or
- monitoring individuals in a workplace

58. The above scenarios are unlikely to occur in relation to the use of BWV, save for the first example. The remaining two scenarios are more applicable to the Council's use of CCTV.[35] If a DPIA is undertaken, the Council will consider both the likelihood and the severity of any impact on individuals and the reasonable expectations of the individuals whose personal data is processed and the potential impact on their rights and freedoms.

59. The considerations and mitigations must be included in the DPIA prior to any deployment of a surveillance system that is likely to result in high risk to individuals. If high risks cannot be mitigated, prior consultation with the ICO is required.

60. Guidance as to what the DPIA should contain is found in the ICO's Video Surveillance Guidance,[36] along with a DIPA template or Surveillance Cameras[37] and guidance for conducting DPIAs.[38] Similarly, if the Council determines a DPIA is not required, the reasons the processing is not of a type likely to result in high risk must be documented.[39]

PROCESSING PERSONAL DATA

61. The Council must ensure the personal data processed from the BWV is:

- adequate - sufficient to properly fulfil the stated purpose;
- relevant - has a rational link to the purpose; and
- limited to what is necessary - you do not hold more than you need for that purpose

FAIR PROCESSING OF DATA

62. The Data Protection Act 2018 requires that the data subject must be informed of:

- the identity of the data controller;
- the purpose(s) for which the footage is intended to be processed; and
- any further information that is necessary for processing to be fair.

RETENTION

63. Once the recording has been completed, it is potential evidence for use in an investigation/ prosecution and/or complaint. All images from BWV have the potential for use in court proceedings, whether they provide evidence helpful to the prosecution or defence. The

[35] https://www.eastleigh.gov.uk/media/2585/cctv-code-of-practice-2016.pdf
[36] https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-0-0.pdf
[37] **Appendix 3**
[38] https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf
[39] ICO's Video Surveillance Guidance – Screening Checklists

BWV product must therefore be safeguarded by an audit trail in the same way as other evidence retained for court, to ensure the defendant has a right to a fair trial.[40] Once it becomes clear the purpose for which the images were taken is no longer valid or no longer exists, the possibility the photographs could be of some legitimate use in the future is generally insufficient to justify continuing retention.

RETENTION PERIOD

64. There is no prescribed minimum or maximum retention period for surveillance systems, or the personal data processed from the recorded product. Instead, it is the purpose of the processing that should determine the retention period. In order to provide sufficient time for checks to be undertaken as to whether the footage is required for an investigation, prosecution, complaint, or appeal, the shortest time and therefore minimum period the Council initially requires retention of the footage is **6 months.**

RETENTION CHECKS

65. During the **6 month** retention period, officers must take all reasonable steps to ensure the recorded material (images, video and/or audio) is not required as evidence in any investigation/prosecution/complaint, in order to determine if and how long to retain the material for. If the retention check confirms the footage is <u>not</u> required as evidence, it must be deleted once the decision is made. If the footage <u>is</u> required as evidence, it must be retained beyond the **6 month** retention period for a period determined by whether it is an investigation or prosecution and in accordance with Disclosure obligations.

STORAGE OF DATA

66. Recordings must be securely held in accordance with the Council' storage procedures, in order to maintain the confidentiality, integrity and availability of the information to ensure the Council protects the rights of the individuals recorded by the BWV and can use the information effectively for its intended purpose. Video recordings must not be tampered with, lost, or accidentally destroyed. Images should be stored and retained so they are retrievable and accessible for replay and viewing and kept in an environment that will not be detrimental to the quality or capacity for future viewing. The information should be stored in a way that makes it easy to identify, locate and retrieve relating to a specific individual or event.

RESTRICTED ACCESS & DATA ENCRYPTION

67. Access to the BWV's recorded product is restricted to the Council's BWV Officers[41] and video recordings should be protected if the device is lost. Both the Information Commissioner's Office (ICO) and Biometrics & Surveillance Camera Commissioner (SCC) recommend encryption as an effective way to achieve data security.

68. The image file or indeed the whole drive can be encrypted so that the file cannot be opened except with the correct decryption key. This has particular value if images are to be transmitted to or from remote sites. Encryption does not change the data contained within the file. Loss or corruption of the encryption key may make files unrecoverable. Encryption

[40] ECHR Article 6
[41] **Appendix 4**

systems that progressively decrypt on demand, rather than decrypting the whole file prior to replay may affect image quality on replay systems with low processing power.

69. Some systems will employ a form of encryption known as Digital Rights Management (DRM) that prevents access to the file without the correct credentials.

DATA PROTECTION PRINCIPLES FOR HANDLING DIGITAL IMAGES & EVIDENCE

70. The following data protection principles[42] are most relevant when handling digital images and evidence:

- Principle 3 (Relevance) - Data must be adequate, relevant, and not excessive in relation to the purpose for which it is processed.
- Principle 5 (Retention) - Data should only be retained for as long as it is necessary for the purpose it was originally collected. Policies should be in place setting out standard periods of retention.
- Principle 6 (Security) - Appropriate security measures should be in place to protect personal data.

71. It should be noted that the requirements of Principle 5 (Retention) must be harmonised with the retention requirements in the CPIA and Information Management.

72. Images should also be protected from accidental deletion by the careful handling of media. Media should be stored in clean, dry environments and kept away from strong magnetic fields, strong light and chemical contamination.

SECURITY MEASURES

73. The Council's implementation of appropriate technical and organisational security measures includes:

- any ability to make copies of information is restricted to appropriate staff;
- ensuring that there are sufficient controls and safeguards in place if the system is connected to or made are available across a network;
- where information is disclosed to a third party, it can be safely delivered to the intended recipient
- control rooms and rooms where information is stored are secure;
- training staff in security procedures with sanctions against staff who misuse surveillance system information
- awareness of staff that they could be committing a criminal offence if they misuse surveillance system information;
- being aware of any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied to the Council's system or any other devices connected to it or both

74. The Council will document procedures and review them annually in conjunction with the annual review of this Policy.

PERIODIC REVIEW OF SYSTEM

[42] Data Protection Act 2018, Part 3, Chapter 2

75. The Council will undertake a periodic review every quarter of its BWV system's effectiveness to ensure it is still doing what it was intended to do. Further, CDs, DVDs, digital tapes and so on are designed for short-to-medium term storage periods. To ensure the integrity of the data the files need to be transferred to new media regularly, possibly as often as every 5 years, or transferred to professionally managed data management archive systems. Data on these systems needs periodic review to ensure that the format is still accessible with currently available software and codecs

DELETION/DISPOSAL

76. The Council has measures in place to ensure the permanent deletion of information through secure methods. No image obtained for the purpose of an investigation should be deleted without authority and completion of audit trails should be undertaken once statutory retention periods are completed, in accordance with the Council's Data Retention Policy[43].

PRIVACY INFORMATION

77. In addition to requiring clear signage, verbal announcements, or lights/indicators on the device itself, the ICO requires a readily available Privacy Policy accessible on the Council's website. If appropriate, the BWV user should direct the individual to the Council's Privacy Notice and Local Area Services Privacy Policy.[44]

TECHNICAL GUIDANCE FOR BODY WORN VIDEO DEVICES

78. The Council has also considered and incorporated the Home Office Technical Guidance for Body Worn Video Device [45] along with the recently published ICO Video Surveillance Guidance which has to an extent superseded the Home Office Technical Guidance. The Council has also considered and incorporated the Home Office Digital Imaging & Multimedia Procedure (DIMP) V3[46] (16 November 2021) into this Policy.

STORAGE OF EQUIPMENT

79. When equipment is not in use, it should be securely stored in a suitable Council location. Each BWV Officer is assigned a BWV device which is electronically assigned to the BWV Officer during the "Booking Out," process. This process includes the option to retain the booked out user and also automatically creates an electronic contemporaneous issue and returns log when the device is taken or put back into the docking system.

DURABILITY

80. Devices should be suitably robust and function effectively in their operational environment.

---

[43] https://staffhub.eastleigh.gov.uk/s/article/Retention-and-disposal-schedule

[44] https://www.eastleigh.gov.uk/privacy ; https://www.eastleigh.gov.uk/privacy/privacy-notices-for-service-areas ; https://www.eastleigh.gov.uk/media/3925/cctv-privacy-notice.pdf

[45] Published July 2018, Publication No 012/18 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746287/technical-guidance-body-worn-video-01218p.pdf

[46] https://www.gov.uk/government/publications/digital-investigations-digital-imaging-and-multimedia-procedure/digital-imaging-and-multimedia-procedure-v30

INTEGRITY

81. The user should be confident the device has correctly produced the recording. Further, one of the fundamental requirements of digital imaging is the need to safeguard the integrity of images; part of this process involves an audit trail being started at the earliest stage. This may be as a written audit trail, and/or incorporate an auto-generated electronic audit trail mapping the movement and changes of files on computers. When relating to third party images, the audit trail should begin at, and detail, the point of transfer.

82. The audit trail may be written and/or incorporate an auto-generated electronic audit trail mapping the movement and changes of files on computers. The audit trial should include the following information (with date and time of action) when available and if appropriate:

- details of the case;
- classification of the image(s) (and any special handling instructions, if relevant) and the name of the person who classified the image;
- if the image is third-party generated, information about point of transfer including whether the image is the Master, a Working Copy or an exhibit derived from a Working Copy;
- information about capture equipment and/or hardware and software used, including details of the maintenance log relating to capture equipment and calibration of hardware and software;
- Licence Identity of the capture operative including third parties and image retrieval officers, where applicable;
- Where third party data is requested:
    - letter to third party
    - explanatory note
    - third party response letter
- details of exhibits and disclosure officer(s);
- description of the images captured, including sequencing;
- details of retrieval or seizure process and point of transfer, if applicable;
- creation and defining of the Master Copy and associated metadata;
- storage of the Master Copy;
- any access to the Master Copy;
- viewing of the Master and Working Copies, including a record of any associated viewing logs;
- details and reasons for any selective capture;
- any editing applications which may alter the image;
- any details of processing applications allowing replication by a comparatively trained individual;
- electronic history log of processing applications;
- any copying required to ensure preservation and longevity of the data;
- revelation to the CPS of the Master and Working Copies;
- any copying carried out as part of a migration strategy to ensure the replay longevity of the image;
- disposal details and retention time periods;
- hash value or equivalent at point of receipt;
- reason for collection or receipt of the imagery

DATA TRANSFER TO BACK OFFICE SYSTEM

83. Video recordings should be transferred off the device as soon as is possible.

84. The Council's BWV system provides the option to allocate Personal Issue during the Booking Out process (see para. 79) and all BWV Officers are required to use the Personal Issue option. The BWV footage is downloaded onto a secure system when placed back into the docking station. The system identifies during the data transfer uploading process the status of the upload via its progress bar and visual images. Once complete the device indicates "Upload Complete," following which the footage will automatically be deleted from the device.

VIDEO DATA

85. To facilitate the use of the recordings for investigations and appeals and so on, the video data should be part of a package, containing the following information:

- clear identification of the image sequence or sequences
- an easily-read text file stating any requirements for special hardware or software for replay
- all associated metadata (time and date should be bound to the relevant images)
- licence-free software enabling the sequences to be viewed correctly

86. Other items that could be included:
- text data about the originating camera or system
- audit trails
- authentication or verification software
- short test sequence to confirm that the recorded image sequences are being replayed correctly
- Contact details for the Council's Data Protection Officer in case of media being lost / found

87. The Council's BWV system deals with these requirements by providing the following electronic audit trails:

FEATURE	**SUMMARY**
Audit Log	Filter option by date range, user or action
Booking Log	Who booked out, location, personal issue or not
Reports	Model, date added to DEMS 360, date decommissioned if Applicable, last recording date, last booking date, current booking date, booker user and allocated location if applicable
Camera Booking Log	Activity for every camera, booking state, user, location and full booking history
User's Activity	Number of uploaded files, deleted files, burned files, exported files and snapshots created
User's Uploading Statistics	Count of following files: non-evidential, evidential, deleted, total, Total duration and total size

STILL IMAGES

88. In general, still images are stored in widely supported formats and there is no need for viewing software to be stored with the images, but where proprietary formats are used then the viewing software should be included on the media in line with the information given above for sequences.

REUSABLE MEMORY

89. The Council's BWV system process to transfer data from the device to the system is set out above (see paragraph 83-84). Once images are transferred the reusable medium is automatically reformatted/sanitized to remove all of the previous image files in preparation for reuse.

NETWORK

90. The Council's BWV system network is Reveal DEMS 360.

BODY WORN VIDEO PROCESSES

91. A staff user guide[47] has been produced, using the relevant information from this Policy to facilitate BWV Officers use of BWV and ensure compliance with the relevant legislation.

PRE-LAUNCH ADVERTISING

92. The Council will commence a pre-launch advertising campaign by publishing details on EBC's website[48]. This will inform the residents and businesses within the Borough that the Council intends to launch use of BWV devices by authorised officers.

UNIFORM & POSITIONING OF BWV

93. The Council's use of BWV will be reiterated by officers wearing a symbol/sign on their uniform. Further, the BWV device will be in a prominent position (normally on their chest) and the officer will ensure that its forward-facing display is visible to persons being recorded.

START OF SHIFT PROCEDURE

94. All BWV Users will be issued with their own device at the commencement of their shift and the device's electronic Booking Out process will be completed to identify the user.

MAINTENANCE OF EQUIPMENT

95. The user must ensure the equipment is in working order before commencing duty and any malfunction of equipment must be reported.[49] These checks should ensure:

- the unit is correctly assembled;
- recording picture is the right way up;

[47] **Appendix 5**
[48] Insert link to Website page
[49] To be reported to Parking Operations Team Leader) or Local Response Officer Team Leader

- sound recording level is appropriate to use and the system date and time stamp is accurate**.** operator adjustable settings are made appropriately;
- the system time and date settings are correct;
- if the equipment is battery operated the internal battery is fully charged;
- a scheme of checks is carried out before deployment particularly for equipment that is used less frequently

96. It is essential that time and date settings are correct. Any inconsistencies should be documented, and the equipment monitored to ensure that further drift of these settings does not occur.

DECISION TO RECORD AN INCIDENT

97. Recordings must be incident specific and should only be made in situations where the BWV user would previously have made a written record of the encounter for example in their pocket notebook and/or within a statement. BWV users must not record beyond what is necessary for their deployed specified purpose in order to ensure the recording is not excessive.

GENERAL PATROLLING

98. Recordings should not be made of general patrolling duties or entire patrols unless it is part of a specific operation/incident.

AUDIO RECORDING

99. When deciding whether to record the audio content, consideration must be given to the Code's Guiding Principle 2 (Effect on Individual & Privacy) and whether it is proportionate. BWV users should not normally use surveillance systems (BWV) to directly record conversations between members of the public as this is highly intrusive and will require greater justification. The ICO guidance states the BWV user should switch off by default any capability to record audio, to be activated for example by a trigger switch.

100. Audio recordings should only be used when the BWV user has:

- Identified a particular need or issue and can evidence that this need must be addressed by audio recording;
- Considered other less privacy intrusive methods of achieving this need;
- Reviewed the other less privacy intrusive methods and concluded these will not appropriately address the identified issue and the only way to do so is through the use of audio recording.

101. The BWV user should then take additional steps to make it clear to individuals that audio recording is taking place in addition to any visual recording.

WHEN TO START RECORDING

102. Recordings should commence at the start of any deployment to an incident and should continue uninterrupted until the incident is concluded, either because of resumption of normal patrolling or because recording has commenced through another video system (e.g., town centre CCTV).

VERBAL ANNOUNCEMENT PRIOR TO RECORDING

103. Prior to switching on the BWV, the user must wherever possible/practicable verbally announce to the data subject(s) of an encounter of:

- the date, time, and location;
- video and audio recording is taking/is going to take place using BWV;
- purpose(s) for which the footage is intended to be processed/nature of the incident to which the user is deployed;
- confirmation to those present that the incident is now being recorded using both video and audio;
- Any further information that is necessary for processing to be fair.

104. If this is not practicable due to an on-going incident, then the announcement should be made as soon as possible afterwards. Similarly, if the recording has started prior to the user's arrival at the scene of the incident, they should as soon as practicable announce to those present that recording is taking place and that their actions and sounds are being recorded. Announcements should be made using straightforward language such as:

- I am audio and video recording you;
- I am audio and video recording this incident;
- Everything you say and do is being recorded.

BUFFER RECORDING

105. Some BWV devices offer the ability to continuously buffer recording so if the device is turned on, it may also have recorded the previous few seconds. The BWV user must ensure any buffered recording is not excessive and the user only records the amount of footage intended to be captured.

SELECTIVE CAPTURE

106. When recording an incident, it is likely that BWV users will encounter victims, suspects and witnesses as well as recording the visual evidence of the scene. Selective capture is a means by which users may separate encounters with each of these types of persons or occurrence in order to allow for easier retrieval and disclosure at a later time. For example, a Council officer may record an encounter with a witness that includes their name and address, then this section should not be shown to the suspect and/or their legal representative.

BOOKMARKING

107. Bookmarking may not always be practicable and so should only be attempted if the situation is calm and the BWV user is easily able to undertake this technique. Prior to any temporary suspension for the purpose of bookmarking, the user should make a verbal announcement for the purpose of the recording to clearly state the reason for briefly suspending recording. Following the pause, the BWV user should also announce they have recommenced recording. The bookmarking process will be demonstrated on the final whole recording of the incident by a missing section for a few seconds. In creating the master disk exhibit for court, the user must include all bookmarked sections for the incident as one complete master recording of the incident.

VERBAL ANNOUCMENT PRIOR TO ENDING OF RECORDING

108. The user should continue to record for a short period after the incident to clearly demonstrate to any subsequent viewer that the incident has concluded. Prior to concluding the recording, the BWV user should make a verbal announcement to indicate the reason for ending the recording, which should include:

- Date, time, and location; and
- Reason for concluding the recording.

BWV IN PRIVATE DWELLINGS

109. If a BWV user is called to attend a private dwelling, the need to record the incident will have to be far greater in order for the use of the BWV to be both justified and proportionate and the reasoning will have to be evidenced. The requirement for the BWV user to, whenever practicable, make a verbal announcement that recording is taking place is particularly important when in a private dwelling, such as attending a home address regarding a complaint of noise nuisance or anti-social behaviour. The rights of individuals to respect for private and family life[50] must be carefully considered when considering whether to use BWV in a private dwelling, as it is likely to be particularly intrusive, especially during the times of day when occupants are likely to be in bed.

110. BWV users should therefore exercise their discretion and only record when it is relevant to the incident and necessary for gathering evidence, where other reasonable means of doing so are not available and the recording is relevant to the incident.

111. Officers may find that one party objects to the recording taking place, for example where it is a noise nuisance complaint from a tenant in a shared let property. In such circumstances, officers should continue to record while explaining the reasons for recording continuously, such as:

- an incident has occurred requiring Council officers to attend;
- there is a requirement to secure best evidence of any offences that have occurred whether this is in writing or on video, the video evidence will be more accurate and higher quality and therefore it is in the interests of all parties to record it, such as the level of noise created by a shared occupancy tenant playing excessively loud music over a prolonged period, in order to prove the noise is a statutory nuisance;
- 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;
- the incident may reoccur in the immediate future;
- continuing to record will safeguard the officer against any potential allegations from either party;
- any non-evidential material will be retained for a maximum of 6 months only;
- the material is restricted and cannot be disclosed to third parties without the subject's express authority, unless prescribed and permitted by law;
- recorded material is Council information and can be accessed on request in writing in according with Freedom of Information Requests, unless and exemption applies and is also accessible by a subject access request.

[50] Article 8 ECHR

112. If at any point it becomes clear the incident would no longer be the subject matter of an entry in the officer's pocket notebook, then the officer should cease recording. Footage taken in private dwellings should be deleted as soon as is practicable once it has been checked and confirmed it is not relevant to any criminal investigation/prosecution or complaint.

WITNESS FIRST ACCOUNTS

113. If the BWV user is approached by victims or witnesses who are giving their first account of the crime, the BWV user may record the encounter which should be treated as an evidential recording. The first account is principally about determining any action that is immediately necessary. Officers should only ask questions as are necessary to:

- establish if an offence has been committed;
- establish where it occurred and who was responsible;
- assess the current risk to the victim(s) and witness(es);
- identify and prioritise areas of the investigation

114. Such recordings do not replace the need for formal written statements from victims or witnesses but are to be used as supporting evidence. If multiple witnesses wish to give their accounts to a Council officer wearing a BWV, then wherever practicable, witnesses should be kept physically separate to avoid contaminating descriptions or other evidence.

115. The bookmarking process should be adopted so that individual accounts can be easily separated. In addition to producing the footage of the first accounts, officers would also be required to produce a statement of the first account. If the victim does not consent to be video recorded, the BWV user may consider diverting the camera away from the victim, disconnecting the camera or obscuring the lenses and recording the encounter only using the audio facility. The explicit consent of the victim must be obtained prior to beginning either form of the recording.

SCENE REVIEW AND PREMISES SEARCHING

116. BWV can also be used to record the location of objects and evidence at a crime scene and/or during the search of premises.

LIMITATIONS ON USE

117. BWV recordings are not appropriate in certain circumstances such as:

- Legal privilege – e.g., consultation with suspect and his/her solicitor;
- Private dwellings – there must be clear justification for using BWV and the user must not record beyond what is justifiable, lawful, necessary, and proportionate for the evidential requirements of the case;
- BWV should not be used for formal investigative interviews (PACE interviews) with certain witnesses, nor may it be used for interviewing suspects;
- Users should exercise care in using BWV where it may cause serious offence, for example during religious worship

END OF SHIFT

118. BWV users must ensure any BWV footage confirmed during the course of their shift to be required for evidential purposes, is correctly bookmarked and any Incident Report is completed.

119. BWV officers are individually responsible for ensuring their allocated BWV device is correctly connected to the docking station to enable downloading and charging at the conclusion of their shift.

REFERRAL TO POLICE

120. For incidents where the police were not in attendance, a BWV Authorising Officer[51] will review the footage in consultation with the BWV Officer to decide whether a referral to the police is appropriate. If a decision is made not to refer the incident to the police, the BWV footage shall be uploaded in the usual way and retained for 6 months. If a decision is made to refer the incident to the police it is reported via 101, including the fact there is BWV footage. If the police pursue an investigation they request the footage via a DP2 Form; the footage is downloaded from the system onto an encrypted USB, uploaded to the standalone DEMS PC and sent to the police via DEMS. The fact of the police referral is recorded within the Council's Health and Safety Incident Record and therefore it is not necessary to maintain a separate BWV police referral register.

SAFEGUARDING BODY WORN VIDEO DATA

121. The Council has considered and adopted the principles contained in the Home Office Safeguarding Body Worn Video Data.[52]

DATA RECORDED BY BWV DEVICES

122. BWVs record both video and audio content and have wide angle lenses to capture events across a broad field of view, which is likely to result in capturing information that is either not crucial to and/or relevant to the investigation, is deemed collateral intrusion and may additionally be sensitive data. The two categories of information captured by BWV are:

i)	Primary Information	Intentionally recorded and relevant;
ii)	Secondary Information	Unintentionally recorded and not relevant

123. Examples of Primary Information are 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; peoples' physical and mental state/demeanour/ actions; atmosphere during an incident; location of evidence; record of criminal activity. Examples of Secondary Information which is unlikely to be relevant to an investigation are private conversations between officers at the scene of an incident or family photos at the premises of the victim which contains images of the victim's children. This category of

[51] **APPENDIX 2**

[52] Published October 2018 – Publication No.011/18
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746254/safeguarding-body-worn-video-data-01118o.pdf

information may also be sensitive as it relates to Operational Policing; Police and Emergency Personnel; members of the Public.

124. The location of the BWV whilst recording may increase the risk of recording sensitive information such as a hospital, place of worship, private home. BWV users should therefore be aware of their device's potential to capture secondary information, in particular sensitive information and greater discretion may be required when recording in special locations.

CONSEQUENCES OF LOST BWV DATA

125. It is vital all BWV data is securely retained in order to avoid it being lost and/or accessed by unauthorised personnel. Any data breach must be reported to the Data Protection Officer, who will determine if the incident needs reporting to the ICO. Measures which can assist in safeguarding data are:

- Physical security of BWV devices;
- Protecting Data on BWV devices;
- Transferring data to back office system;
- Tagging and organising data;
- Asset management of BWV devices

USE OF MATERIAL AS EVIDENCE

126. When producing any form of digital evidence, it is essential Home Office Digital Imaging & Multimedia Procedure (DIMP) V3[53] (16 November 2021) is followed.

MASTER COPY

127. The Core principle of the Digital Imaging & Multimedia Procedure (DIMP) V3 is the creation of an identifiable, isolated, and suitably stored Master reference copy at the earliest opportunity, known as the Master Copy, which must be stored securely, pending its production (if required) at court in evidence as an exhibit. The exact method of storage is to an extent unimportant, provided it can be shown the Master is unchanged from the moment of its definition in order to confirm the authenticity of the evidence relied upon in proceedings. The Council's Master Copy is currently, and will remain, stored on a separate secure PC with restricted access and the laptop is located in a locked room with restricted access.

128. The Master Copy may be stored as a physical item or purely in digital form. The DIMP guidance acknowledges the benefits of storing both the Master and Working Copy on a secure server instead of a physical WORM (Write Once Read Many) media such as CDs and DVDs. The Council's secure server environment is the Reveal DEMS (Digital Evidence Management System). The Master Copy should not be used, except to produce additional Working Copies when no other Working Copies are available to copy, or by order of the court to establish authenticity.

129. The Master must be:

[53] https://www.gov.uk/government/publications/digital-investigations-digital-imaging-and-multimedia-procedure/digital-imaging-and-multimedia-procedure-v30

- Labelled or named (with due care to the longevity and readability of label and of medium);
- Preserved in a form and manner with software if required, so that the images may be viewed in the future;
- Stored in a manner that prevents alteration or accidental erasure; this can be by either physical or electronic means;
- Kept in accordance with the exhibit protocol;[54]
- Not used, except to make further copies, in whole or in part, together with an appropriate adult trail, or by order of the court to verify authenticity. If viewed directly, suitable write-protection must be in place.

130. The Master should be designated at the point at which the data is under Council control and has been stored according to the conditions described above. There may be intermediate steps between the initial capture and the designation of the Master Copy, involving for example transmission or the use of a transfer medium. There must be an accompanying audit trail showing its provenance. All use and movement of the Master must be logged in the audit trail.

WORKING COPY

131. Officers must create a working copy from the original media for use during the investigation process, for service in evidence and disclosure. The Working Copy is usually produced simultaneously or immediately after the Master is defined and is the version to be used for investigation and to assist in the preparation of the prosecution file, if the matter progresses to commencing criminal proceedings. Significant use, enhancement and distribution of Working Copies should be logged to support the presentation of evidence. If the quality of the original recording (video or audio) requires enhancement, this work should be undertaken using the working copy. At the conclusion of the processing, a copy must be sealed as a master version of the incident post-enhancement. Statements dealing with the technical enhancement process and continuity trail will be required.

132. Working Copies produced for the investigation, technical investigation, briefings, circulation, and preparation of prosecution evidence and defence can be in any of the forms described:
    - digital file;
    - hard copy stills from still or video cameras;
    - edited video;
    - enhanced still or video;
    - converted to non-proprietary format

AUDIT TRAILS

133. All audit trails should be disposed of when image files and any analogue copies are disposed of.

PLAYBACK

[54] See Criminal Procedure & Investigations Act 1996 Code of Practice; Retention, Storage and Destruction

134. Playback will only be permitted and facilitated if formally requested in writing or verbally requested. A playback record is automatically electronically recorded by the Reveal PC software, hence a separate Playback Request Log is not required. If a request is made by a Police Officer attending the incident or by another police officer subsequently involved in the investigation, a playback request log can be generated and produced from the system.

CONTINUITY

135. In order to prove the authenticity and continuity of recordings, officers should produce evidential continuity statements to confirm that any securely stored sealed master copy has not been tampered with. The following content should be included in the statement:

- Equipment serial number/identifying mark;
- Day, date, and time the user took possession of the equipment (time A);
- Day, date, time, and location the user commenced recording (time B);
- Day, date, time, and location the user concluded recording (time C);
- Day, date, time, and location that the master copy was created and retained in a secure storage (time D);
- If any other person had access to or used the equipment between times A, B or C and time D (if so, a statement will be required from that person).

PREPARATION OF A PROSECUTION FILE

136. Officers responsible for file preparation for Legal Services should:

- ensure that the Master is kept in suitable and secure conditions by the Council and copies made available to the prosecution or defence, upon request;
- be cognisant of any redaction requirements where personal data is not to be shared with defence or third parties;
- liaise with the relevant Legal Specialist at an early meeting to discuss the processes and capture systems used, where relevant;
- provide Legal Services with full information accompanying any evidential digital images, this might include audit trails, maintenance logs, viewing logs and disclosure schedules;
- list and describe any unused and/or un-viewed material clearly;
- ensure that viewing logs used for moving images highlight relevant sequences;
- provide Legal Services with accurate information about the preferred format for revelation in order to reduce the loss of image quality;
- consider the format in which the image is provided to Legal Services in order to facilitate viewing and replay;
- liaise with the Legal Specialist to ensure that viewing and replay is possible prior to trial. It should be noted that it is often not practical to play the native format at court

EVIDENTIAL STATEMENTS

137. Any recording of an incident is likely to provide better evidence than an officer's recollection and subsequent pocket notebook note and statement. If the recording covers the whole incident, it is not essential for the officer to produce a statement detailing the entire incident as this is avoidable duplication. If two officers are present at the same

incident, whilst the other officer deals with the incident, the resultant recording can be utilised as evidence for both officers as long as it shows the entire incident. The recording officer should also make notes of the incident to cover any additional points that may be outside the view of the camera as well as all evidential information required in the event of a technical failure.

138. The statement must include details of the evidential audit trail for the production of the master disk, and in order to assist both the prosecution and defence, it is advisable that the statement producing the exhibit contains a summary paragraph outlining the evidential aspects of the incident and the recording.

139. It is recommended the officer records each incident in its entirety from the time of deployment to conclusion. If there is any break in the recording, details, and the reason for this must be included in the officer's statement.

140. BWV users should note that although a recording shows significant detail, some evidential information may take place out of view or hearing of the camera or microphone. It is vital all such additional information is recorded in statements so that the full detail of the evidence is captured. It may therefore assist to provide a running commentary in the video of evidence that you are aware of, but which is not captured, to assist subsequent viewers.

TECHNICAL FAILURE

141. In the event of technical failure of BWV equipment, it is vital the officer is still able to provide the best possible evidence through a traditional witness statement. It is therefore crucial the BWV user remains attentive throughout in order to ensure they can subsequently recall all evidential aspects of the incident within a witness statement. If the equipment has captured part of the incident, it should be produced in evidence and the remainder of the incident be recorded within a witness statement.

EXHIBITS

142. All images should be presented so that evidential content is not compromised. Where possible, images should be presented in their native or original format. If there is pertinent material that can only be seen when the image is viewed in proprietary form then provision should be made for appropriate playback equipment to be provided in court, if these arrangements are not already in place. It should be understood that images may look different depending on the transmission and display equipment used. In particular, images viewed on different screens or by different media players may appear different from one another. An accurate replay facility should be provided wherever possible.

TRANSCRIPTS

143. The BWV footage is produced as an exhibit by the BWV user, hence a transcript will rarely be required, so for example if translation is required or the sound is of poor quality.

REDACTIONS

144. Redactions include editing/censoring/obstructing those parts of a recording that contain collateral intrusion of non-suspects/third parties; sensitive information; expose police tactics or compromise operational strategies. Redactions can be both audio and/or visual. This

may therefore require removing sections of a recording; concealing or masking visible objects such as pixilating photos, blurring, masking or using a solid fill to completely obscure parts of the footage; removing metadata and muting parts of the audio content.

COPIES

145. Copies of footage should be obtained when required, in a timely manner in a suitable format, without losing image quality or time and date information.

THIRD PARTY DATA SHARING REGISTER

146. Any third party request for data must be in writing via a DP2 Form, or if due to the urgency of the situation it may be made verbally. There is restricted access to the BWV system, therefore the process of accessing, viewing, capturing and electronically sending the requested BWV footage to any third party, cannot be dealt with by the Data Protection Team. To ensure records are maintained, all Third Party Data Sharing requests must be recorded firstly in the BWV Team Centrally Retrievable Electronic Third Party Data Sharing Register[55] and secondly, a copy of the DP2 must be provided to the Data Protection Team via email[56], on receipt and prior to it being processed and/or responded to.

DATA SHARING WITH OTHER AGENCIES

147. The Data Protection Act 2018[57] allows the sharing of material with a statutory partner agency where it is necessary to prevent or detect crime or apprehend or prosecution offenders. The Data Sharing Code of Practice[58] was implemented by the Data Protection Act 2018[59] (DPA) and came into force on 5 October 2021. Once any required redactions have taken place, the product of any BWV must not be shared unless it is accordance with a Data Sharing Agreement. Once information is disclosed to a third party, they become the controller for the copy they hold.

148. When providing data to the police, the system should allow the police to:

- take receipt of evidential recordings in order to safeguard them;
- replay the recordings in order to view and copy them;
- make authentic (not materially different) copies in formats suitable for use by investigators, Crown Prosecution Service (CPS) and the courts;
- access viewing facilities if the original recording has to be viewed

149. The Council's method for lawfully providing BWV data to third parties is by either completing the DP2 Request form and providing a physical copy of the data onto an encrypted USB or electronically via a DEMs upload to the police. It is intended that in due course this process will be modified to permit the data to be transferred electronically, enabling a direct link to an external upload to the police.

DATA SHARING WITH THE MEDIA

---

[55] **Appendix 6**
[56] Data Protection Team email – dp@eastleigh.gov.uk
[57] Data Protection Act 2018, Schedule 11, paragraph 2
[58] https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice-1-0.pdf
[59] Data Protection Act 2018 Section 125

150. Sharing of BWV images to the media usually occurs in the course of a police investigation in order to assist in tracing wanted suspects or locating people who have escaped from custody. Circumstances where the Council may wish to release BWV images is for a post-conviction press release. There are specific restrictions to the principle of open justice.

151. Firstly, there is an automatic restriction on reporting information that identified or is likely to identify any person under the age of 18 who is concerned in youth court proceedings as a victim, witness, or defendant.[60] Secondly, there is a discretionary power to restrict reporting the identity of victims, witnesses, and defendants under the age of 18 who appear in Magistrates' Court or the Crown Court.[61]

152. The Council has considered and adopted the **Protocol for working together: Chief Police Officers, Chief Crown Prosecutors, and the Media**[62] to identify and determine Media Access to Prosecution Materials. Prosecution material which has been relied upon (served) by the prosecution in court and which can normally be released to the media includes:

- Maps/photographs (including custody photos of defendants)/diagrams and other documents produced in court;
- Videos showing scenes of crime as recorded by police after the event;
- Videos of property seized (e.g., weapons, clothing as shown to jury in court, drug hauls or stolen goods);
- Sections of transcripts of interviews/statements as read out (and therefore reportable, subject to any orders) in court;
- Videos or photographs showing reconstructions of the crime;
- CCTV footage of the defendant, subject to any copyright issues.

153. Prosecution material which may be released after consideration by the Crown Prosecution Service in consultation with the police and relevant victims, witnesses and family members includes:

- CCTV footage or photographs showing the defendant and victim, or the victim alone, that has been viewed by jury and public in court, subject to any copyright issues;
- Video and audio tapes of police interviews with defendants, victims, and witnesses;
- Victim and witness statements.

154. Where a guilty plea is accepted and the case does not proceed to trial, then all the foregoing principles apply. But to ensure that only material informing the decision of the court is published, material released to the media must reflect the prosecution case and must have been read out, or shown in open court, or placed before the sentencing judge.

PROVIDING COPIES/DISTRUBUTING BWV DATA

155. It will be necessary at times to provide copies of BWV recordings within the Council such as to Legal Services or externally to third parties, including service of evidence to the defence and court. A suitable summary of the evidence will suffice as initial details of the prosecution

[60] Children & Young Persons Act 1933, Section 49
[61] Youth Justice & Criminal Evidence Act 1999 Section 45
[62] Protocol for working together: Chief Police Officers, Chief Crown Prosecutors, and the Media 2005 https://www.cps.gov.uk/publication/publicity-and-criminal-justice-system

case and it should only be necessary to provide copies to the defence in the case of an actual or anticipated not guilty plea. It is important to recognise the master copy of the recorded content is likely to including secondary and/or sensitive information which will require redaction, such as the address of a witness. The redacted version will become the working copy which is the version to be distributed/served.

SERVICE OF BWV PRODUCT

156. Consideration must also be given as to the appropriate form of service of the working copy to safeguard the personal and/or sensitive data contained within it, such as via secure email (cjsm) and/or requiring the recipient to sign an undertaking, if for example the content is graphic. Regardless of the method, personal and/or sensitive data must be protected whilst in transit.

SUBJECT ACCESS REQUEST

157. A Subject Access Request (SAR) is a request by or on behalf of an individual (the Data Subject) either orally or in writing, for either confirmation as to whether the organisation is using or storing their personal information and/or for example, to request a copy of the BWV they are aware filmed the Data Subject.[63] Please note, the BWV may form part of the evidence or unused material in a live investigation/criminal proceedings. Further, the BWV may include third party and/or sensitive data which may require redactions before and in order to facilitate the SAR. In circumstances where it is known there is a live investigation/complaint/criminal proceeding, the council officer with conduct of the SAR **must** refer the request to the Data Protection Officer,[64] to ensure the request does not bypass the evidential or disclosure process and/or prejudice the proceedings. The Council maintains a register of all SAR including those made verbally. This aspect of the Policy should be read in conjunction with the Council's **Subject Access Request Policy**[65] and in accordance with the BWV Third Party Data Sharing set out above, specifying who and how any BWV is to be accessed and provided.

THE RIGHT OF ERASURE

158. Individuals have the right to have their personal data erased,[66] which is also known as the right to be forgotten. This right is not absolute and in the context of surveillance can apply if:

- The information is no longer necessary for the purpose which you originally collected or processed it for;
- You are relying on legitimate interests as your basis for processing, the individual objects to the processing of their information and there is no overriding legitimate interest to continue this processing;
- You have processed the personal information unlawfully (i.e., in breach of the lawfulness requirement); or
- You have to erase it to comply with a specific legal obligation

[63] UK GDPR Article 15(1)
[64] Denise Johnson & Claire Brown
[65] https://staffhub.eastleigh.gov.uk/s/article/Data-Subject-Request-policy
[66] UK GDPR Article 17(1)

159. There are circumstances where the right to erasure cannot be exercised as certain exemptions apply. In the context of surveillance, this may include but it is not limited to:

- Processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
- Certain research activities; or
- Compliance with a specific legal obligation to process surveillance information

THE RIGHT OF RESTRICTION OF PROCESSING

160. Individuals have the right to restrict the processing of their personal data in certain circumstances,[67] so can limit the way in which their data is used, as an alternative to requesting the erasure of their data. In the context of surveillance footage, this may be because they have issues with the content of the information the Council holds or how it has processed their data. In most cases, the Council will not be required to restrict an individual's personal data indefinitely but will need to have the restriction in place for a certain period of time. The ways in which data can be restricted are:

- Temporarily moving the data to another processing system;
- Making the data unavailable to users; or
- Temporarily removing published data from a website

SAR GUIDANCE CHECKLISTS

161. The Home Office Safeguarding Body Worn Video Data (2018) contains the following helpful checklists for the Data Controller[68]:

- SAR Checklist for Data Controller;
- Visual Data Redaction – Disclosure Requirements
- Visual Data Redaction Considerations;
- Visual Data Redaction Techniques;
- Audio Data Disclosure Requirements;
- Audio Data Redaction Considerations;
- Audio Data Redaction Techniques;
- Output Video and Audio Data Considerations

FREEDOM OF INFORMATION REQUESTS

162. The Freedom of Information Act 2000 provides the public a general right of access to all types of recorded information held by public authorities, which may include the digital and audio content recorded by BWV devices. Public authorities include local authorities and recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings. There are two exemptions to relating to the information about individuals[69]:

- Is the information personal data of the requester? If so, then that information is exempt from FOIA and instead the requester should make a Subject Access Request (SAR);

[67] UK GDPR Article 18(1)
[68] **Appendix 7**
[69] Freedom of Information Act 2000, Section 40

- Is the information personal data of other people? If so, then the Council will only disclose the information if:

❖ First condition disclosure does not contravene one of the data protection principles;
❖ Second condition disclosure does not contravene an objection to processing; and
❖ Third condition the information is not exempt from the right of access

163. The Act does not give people access to their own personal data (information about themselves) such as their health records or credit reference file. If a member of the public wants to see information that a public authority holds about them, they should make a data protection subject access request (SAR).

EXEMPTIONS TO FREEDOM OF INFORMATION REQUESTS

164. Exemptions to the requirements to disclosure information include:

- National security[70];
- Investigations or proceedings[71];
- Law enforcement[72];
- Personal information[73]

UNLAWFUL DISCLOSURE TO THIRD PARTIES

165. It is an offence[74] for a person, knowingly or recklessly, –

(a) to obtain or disclose personal data without the consent of the controller
(b) to procure the disclosure of personal data to another person without the consent of the controller; or
(c) after obtaining personal data, to retain it without the consent of the person who was the controller or in relation to the personal data when it was obtained.

166. These offences are triable either way and punishable by way of a fine[75]. The statutory defences available are contained in Section 170(2) and (3) of the Data Protection Act 2018.

DISCLOSURE DUTIES & OBLIGATIONS

167. In addition to considering document storage, retention and destruction, officers must also consider their Disclosure Duties & Obligations. The statutory framework for disclosure is Criminal Procedure & Investigations Act 1996, Criminal Procedure & Investigations Act Code of Practice[76] & Surveillance Camera Code of Practice.[77]

[70] Freedom of Information Act 2000, Section 24
[71] Freedom of Information Act 2000, Section 30
[72] Freedom of Information Act 2000, Section 31
[73] Freedom of Information Act 2000, Section 40
[74] Data Protection Act 2018, Section 170(1)
[75] Data Protection Act 2018, Section 196(2)
[76] Last revised 2015
[77] Surveillance Camera Code of Practice, Revised November 2021

168. There is a duty to record, retain and review material created and/or obtained during an investigation, which includes retaining both the used and unused images/audio content of BWV recordings. The Disclosure Officer (DO) is responsible for disclosure within the investigation. Their disclosure obligations begin at the start of the investigation, and it remains a continuing duty to conduct a thorough investigation and manage all material appropriately. There is also a duty to follow all reasonable lines of inquiry whether they point towards or away from a suspect.

169. Unused material is material that is **relevant** but does not form part of the prosecution case. Relevant material **is *anything that appears to have some bearing on any offence under investigation, or any person being investigated, or on the surrounding circumstances unless it is capable of having an impact on the case*.**

170. The DO has a duty to review unused material and compile Disclosure Schedules containing Unused Material. There are two types of Schedules of Unused Material. Firstly a Schedule of Non-Sensitive Unused Material[78] which is disclosable to the defence and must be provided to the defence either as part of Initial Disclosure and thereafter subsequent schedules or updates provided to the defence. The second is the Schedule of **Sensitive** Unused Material,[79] which is not disclosable to the defence due to its contents.

171. In compiling the schedules, the DO must assess each item to determine if it meets the **Disclosure Test**. The Disclosure Test requires the prosecution to provide the defence copies or access to any material which might reasonably be considered capable of undermining the prosecution case and/or assisting the defence, which has not been previously disclosed.

172. Once the relevant Schedules of Unused Material have been provided, the prosecutor has a duty to review the schedules and relevant documents, in particular the authorisation and supporting documents. If it is determined the material does not assist the defence or undermine the prosecution case, there is no requirement to disclose the material to the defence.

173. If BWV footage meets the disclosure test, consideration must be given as to whether any redactions are required in relation to, for example, members of the public, other family members who are not the subjects of criminal proceedings. Please therefore follow the Redactions guidance above.

ADDITIONAL REQUIREMENTS

HEALTH & SAFETY

174. To ensure the health and safety of Council staff, each team has specific Risk Assessments and Safe Systems of Work for the duties they carry out within their roles. These are reviewed at least annually and updated as required, in accordance with the Council's overarching **Health & Safety Policy**.[80]

PUBLIC SECTOR EQUALITY DUTY

[78] Form MG6C
[79] Form MG6D
[80] https://staffhub.eastleigh.gov.uk/s/article/Health-and-Safety-Policy

175. The Public Sector Equality Duty (PSED) requires public bodies to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations between different people when carrying out their activities. The Council undertakes Equality Impact Assessments (EqIA) as a tool to assess how the Council functions and how its policies and decisions might impact on certain groups of people with protected characteristics, to ensure they do not discriminate against or disadvantage people. The EqIA ensures and demonstrates the Council has due regard to its statutory duties. The Council has undertaken an EqIA in relation to this Policy.

OVERSIGHT

APPROVAL OF POLICY

176. The Council's Body Worn Video Policy and Processes is submitted to the Audit & Resources Committee for consideration and then to Cabinet for its approval.

ANNUAL REVIEW OF POLICY

177. This Policy will be reviewed annually by the Legal Services Manager.

INTERNAL MONITORING

178. The BWV Authorising Officers will undertake internal reviews of the procedure, system and practice to ensure its fit for purpose not less than quarterly and any issues identified will be notified to all BWV Authorising Officers for their consideration as to what if any remedial steps are required.

COMPLAINTS

179. The Council's Corporate Complaints Procedure is published on its website.[81] In addition, all reported complaints of the Council's use of BWV will be reported annually to the Audit and Resources Committee.

TRAINING

180. BWV Officers will receive training in the relevant technical aspects of the specific equipment being used. This includes for example, assembly (where necessary), day to day use, the capabilities of the devices including how to keep devices and data secure, how to download data to the Council's system, automatic deletion of the data once downloaded to the system, to ensure BWV users inform individuals that recording may take place if it is not obvious to the individuals in the circumstances and to respond to queries and requests from the general public. Additionally, BWV current and intended officers have received Conflict Awareness training. The BWV Authorising Officers maintain a Training Register[82], and only authorise BWV Officers use of the equipment once they have received the relevant training.

THE INFORMATION COMMISSIONER

[81] https://www.eastleigh.gov.uk/council/customer-care/our-complaints-procedure
[82] **Appendix 8**

181. The Information Commissioner is the UK's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals. The Information Commissioner has a broad range of statutory duties, including monitoring and enforcement of the GDPR, promotion of good practice and adherence to the data protection obligations by those who process personal data. These duties are in addition to the specified statutory regimes the Information Commissioner is empowered to take a range of regulatory action for breaches.

THE BIOMETRICS & SURVEILLANCE COMMISSIONER

182. The Biometrics & Surveillance Commissioner[83] is the UK's Independent regulator for upholding the use of overt surveillance camera systems by relevant authorities, including local authorities, in England and Wales. The functions of the Biometrics & Surveillance Commissioner include encouraging compliance with the Code; reviewing the operation of the Code; and providing advice about the Code (including changes to it or breaches of it) and publish an annual report.

MISCELLANEOUS

POLICY REVISION HISTORY

REVISION	REVISION DATE
1	June 2022
2	August 2022
3	

[83] Fraser Sampson appointed 1 March 2021