

Surveillance Processes Body Worn Video

DAERA Inland Fisheries Group adopts the following 12 guiding principles in relation to the use of overt Body Worn Video (BWV), CCTV and Trail Camera operations, as per the Home Office Surveillance Camera Code of Practice:

1. 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.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. 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.
4. 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 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. 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. 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. 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. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. 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. 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. 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.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

Surveillance Processes Body Worn Video

DAERA Inland Fisheries Group adopts the 8 guiding principles of The Data Protection Act in relation to the use of overt Body Worn Video (BWV) and Trail Camera operations

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Surveillance Processes Body Worn Video

The Data Protection Act 1998

SCHEDULE 2 CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1The data subject has given his consent to the processing.

2The processing is necessary—

(a)for the performance of a contract to which the data subject is a party, or

(b)for the taking of steps at the request of the data subject with a view to entering into a contract.

3The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4The processing is necessary in order to protect the vital interests of the data subject.

5The processing is necessary—

(a)for the administration of justice,

[F1(aa)for the exercise of any functions of either House of Parliament,]

(b)for the exercise of any functions conferred on any person by or under any enactment,

(c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d)for the exercise of any other functions of a public nature exercised in the public interest by any person.

Surveillance Processes Body Worn Video

The Data Protection Act 1998

SCHEDULE 3 CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1The data subject has given his explicit consent to the processing of the personal data.

2(1)The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2)The **[F1 Secretary of State]** may by order—

(a)exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3The processing is necessary—

(a)in order to protect the vital interests of the data subject or another person, in a case where—

(i)consent cannot be given by or on behalf of the data subject, or

(ii)the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b)in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4The processing—

(a)is carried out in the course of its legitimate activities by any body or association which—

(i)is not established or conducted for profit, and

(ii)exists for political, philosophical, religious or trade-union purposes,

(b)is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c)relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d)does not involve disclosure of the personal data to a third party without the consent of the data subject.

5The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6The processing—

(a)is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b)is necessary for the purpose of obtaining legal advice, or

(c)is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Surveillance Processes Body Worn Video

7(1)The processing is necessary—

(a)for the administration of justice,

[F2(aa)for the exercise of any functions of either House of Parliament,]

(b)for the exercise of any functions conferred on any person by or under an enactment, or

(c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2)The **[F3 Secretary of State]** may by order—

(a)exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

[F47A(1)The processing—

(a)is either—

(i)the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or

(ii)any other processing by that person or another person of sensitive personal data so disclosed; and

(b)is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2)In this paragraph “an anti-fraud organisation” means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.]

8(1)The processing is necessary for medical purposes and is undertaken by—

(a)a health professional, or

(b)a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2)In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9(1)The processing—

(a)is of sensitive personal data consisting of information as to racial or ethnic origin,

(b)is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

Surveillance Processes Body Worn Video

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The **[F5 Secretary of State]** may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10 The personal data are processed in circumstances specified in an order made by the **[F6 Secretary of State]** for the purposes of this paragraph.

Surveillance Processes Body Worn Video

Privacy Impact Assessment – Use of Body Worn Video by Fisheries Officers

It is widely known that the public, in going about their daily lives, are likely to have their movements and identities captured on a variety of surveillance systems and of paramount importance is to provide proper mitigation to minimise intrusions of privacy.

This Privacy Impact Assessment has been written to explore these issues and in particular to explain;

The rationale for DAERA Inland Fisheries introducing and using this technology.
The legality behind its use.

The likely operational circumstances when Fishery Officers may use it. The key **privacy issues** and **risks** and provides an explanation as to how these will be mitigated.

DAERA Inland Fisheries will continue to monitor the use of the equipment and revisit the Privacy Issues and Risks through ongoing consultation whilst responding to any national and legislative changes.

Purpose of Privacy Impact Assessment (PIA)

Any project or set of new processes that involve exchanging personal information, inevitably gives rise to privacy concerns, from the public. Indeed, the cumulative effect of many such initiatives during recent decades has resulted in harm to public trust and to the reputations of government bodies.

What is meant by privacy?

The Information Commissioner's Office *Conducting Privacy Impact Assessments code of practice* describes privacy in the following way:

Privacy, in its broadest sense, is about the right of an individual to be left alone. It can take two main forms, and these can be subject to different types of intrusion: Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

The Privacy Impact Assessment is a process which helps organisations to anticipate and address the likely privacy impacts of projects, in order that problems can be foreseen and solutions developed to ensure that concerns are addressed appropriately.

DAERA Inland Fisheries has introduced the use of cameras that are capable of capturing both moving images and audio information which will be worn overtly by Fishery Officers.

Surveillance Processes Body Worn Video

The devices will be/have been used in an enforcement and investigatory situation and the aim of undertaking this PIA is to explain the extent of their use, their limitations, how any data captured will be processed coupled with an analysis of the rights to privacy of citizens and the risks posed.

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

What is Body Worn Video?

Any style of video camera deployed by DAERA Fishery Officers, which are overtly carried or fixed to the body of officers which are capable of capturing both video and audio information falls under the category of Body Worn Video.

The devices themselves will be generally mounted on an officer's chest. The equipment will be used in overt regulatory activities.

Why use BWV?

DAERA Fishery Officers are responsible for enforcing The Fisheries Act 1966 (Northern Ireland) As Amended. This involves the investigation, prevention and detection of offences under The Act and in regulatory duties to protect the Inland and Migratory fisheries within the DAERA area. This may involve stopping, speaking and interviewing the angling public, on occasion conducting searches of vehicles, premises, vessels and bags. This also involves the regular recording information in official notebooks (PNB's). In some instances, the rigour of what has been recorded may be the subject of interpretation and the subject of debate. Equally it may not have presented the best possible primary evidence to support a prosecution. By the introduction of this type of technology, the devices themselves are able to record exactly what happened, what was said and when, in an indisputable format. Their use will be at the discretion of an officer and should be: Incident specific, Proportionate, Legitimate, Necessary, and Justifiable.

Using BWV at incidents can enable officers to present their evidence in a consistent and accurate manner. The recording can be produced as an exhibit and therefore the officer has to spend less time recording the incident as a statement or in their pocket notebook.

Another timesaving effect of BWVs is a predicted increase in guilty pleas, resulting in less time spent preparing court papers and attending court. BWV recordings may also be used in any incident where complaints are made about an officer's actions.

In a number of situations past evidence has established that complainants have reconsidered their complaint after reviews of footage, thus reducing unwarranted complaints.

BWV is also a valuable training aid for fishery officers. The ability to review their own performance in detail after an incident, is a powerful tool for officers to highlight effective and ineffective actions. When reviewing their evidence, experienced officers can also use the devices to assess their behaviour and can professionalise their performance accordingly.

Fishery Officers have traditionally used their official notebooks to record key information when dealing with a member of the angling public or capturing initial information at an incident. BWV devices will save time, but importantly must be seen

Surveillance Processes Body Worn Video

as being complementary to any entry being made in notebooks and is not a replacement for it.

This equipment may therefore be used to record video and audio information of encounters between officers and the angling public, (*after ensuring appropriate safeguards in respect of the necessity, legitimacy and legality are addressed - see later*) in respect of: the prevention and detection of fisheries offences, reducing any incidence of public disorder, aggression, intimidation and the assault of officers conducting official duties, to present evidence to bring successful prosecutions before the courts, to provide greater transparency in the working practices of Fishery Officers.

The following categories of citizens may have their contact with fisheries officers, recorded: witnesses of illegal fishing activity or other offences under relevant fisheries legislation, persons suspected of committing fisheries offences and potentially although unlikely victims who have suffered damage or loss as a result of fisheries offences

In addition, persons, unrelated to any specific interaction between fishery officers and any of the categories of persons above, might find their activities captured on a BWV device. To some degree, this is inevitable since a camera lens or microphone is non-discriminatory and captures what is seen or heard. In such circumstances, DAERA adopts a number of safeguards to avoid this wherever possible.

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

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

Added to this, current technology is incapable of operating in such a way principally due to a lack of suitable battery life. In addition, such a practice would require the storing, reviewing and then disposal of large quantities of data.

The equipment will be worn by fishery officers who are on duty, and the use will be primarily driven by the incidents and circumstances presented to them or in anticipation of responding to a reported and unfolding incident, or when exercising a specific power as convened under fisheries legislation.

Surveillance Processes Body Worn Video

General Operating Procedures

The equipment is issued on a personal basis. A set of operational protocols issued by DAERA Inland Fisheries, complemented by the instructions from the respective device manufacturer will be complied with, which ensures device encryption, restricted and secure data access, and automated deletion of any non essential footage. The device will then be overtly attached to the officer with a chest harness. During the course of their normal patrol duties, the device remains in an inert state and therefore is not recording any material. In order to do so, requires the officer to deliberately activate the device to a record mode and where practicable, make a verbal announcement to indicate that the BWV equipment has been activated. This announcement should be present on the recording and if possible, should include: The date, time and location; the nature of the incident to which the user is deployed; and confirmation to those present that the incident is now being recorded using both video and audio.

If the recording has commenced prior to their arrival at the scene of an incident the officer should, as soon as is practicable, announce to those persons present that recording is taking place and that their actions and sounds are being recorded. Announcements should be made using straightforward language that can be easily understood by those present.

At the conclusion of any incident, the record mode on the device is switched off and the captured information is stored.

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

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

Recorded information cannot be deleted or altered using onboard device software and is also fully encrypted as mentioned

At the end of a period of duty, the fishery officer securely stores the device identifying the elements of any captured data that need to be retained to assist in an investigation, and 'marks' the relevant section appropriately, by using the built in software. A regular process of device docking has been put in place by nominated management staff and following this process the officer 'checks in' the device, where it will be "docked", automatically downloading all captured information on to a secure standalone computer with restricted access. This information cannot be deleted or altered without specific managerial authorisation. Once completed, the content on the device is fully erased. All information captured and downloaded will be retained as mentioned on a secure computer.

Any material required to support an on-going investigation or prosecution will be retained as part of the ongoing investigation or case file in relation to the commission of a suspected offence(s).

Further reassurance is provided in that all devices are encrypted and contain built in deletion software which will automatically delete all "non marked" material after a specified period of 31 days. Access to recordings will be controlled and only persons having an operational need to view specific incidents may do so.

Surveillance Processes Body Worn Video

Where information is captured for use in any investigation, once downloaded on to the nominated secure computer, a master copy (*a bit-for-bit copy of the original recording, which is stored securely, pending its production {if required} at court as an exhibit*) of the entire information will be created and a working copy (*the version produced from the original media for the investigation, briefings, circulation, and preparation of prosecution evidence and defence*) of this is then made available. Any information shared with the nominated branch solicitors to assist in any prosecution, will be strictly controlled.

In order that BWV evidence is admissible in court, DAERA Inland Fisheries follows the principles contained in the **ACPO/Home Office (2007) Digital Imaging Procedure v2.1** and the **ACPO (2007) Practice Advice on Police Use of Digital Images**.

The law surrounding BWV

The use by officers of BWV must be shown to be proportionate, legitimate, necessary and justifiable.

In addition, use of the equipment should address a 'pressing social need' especially in respect of its application within the confines of the Articles enshrined by the European Convention of Human Rights within the Human Rights Act 1998. This next section explains the various aspects of the legislation and guidance that covers this equipment, and how DAERA Inland Fisheries will ensure that the rights and privacy of the public are balanced against the law.

There may be occasions where an officer wishes to record an encounter to evidence their own actions; there must be a legitimate reason to this decision, and the recording cannot be used for the sole purposes of aiding the identification of an individual, as this has been held to be unlawful. The decision to record in these circumstances needs to be taken in line with the principles of data management and record retention. Officers should be prepared to account for their decision-making in such instances.

Justifiable purpose within the context of fisheries includes:

- Preserving Order
- Preventing the commission of offences
- Documentation of suspected offences committed
- Other duties arising as a part of statutory powers under fisheries legislation

Legality under Common Law

It has been accepted, that police officers are able to rely on the fact that the use of BWV is deemed to be lawful under Common Law. Police officers are also held to be 'citizens in uniform' although granted additional statutory powers in order to execute their duties. In addition, police officers generally do not require special statutory powers to undertake any activity that the public could lawfully undertake.

Consequently and similarly then fishery officers, when conducting official duties, can legally employ the use of BWV.

The taking of photographs, and in its wider sense video or sound recordings, is deemed lawful and Common Law does not prevent this activity in a public place.

Human Rights Act 1998

Surveillance Processes Body Worn Video

The use of BWV is viewed as 'an interference' and must always be justifiable. Therefore any actions by officers must have a legitimate aim and the use of this equipment must be shown to be proportionate to achieving this.

Under this legislation a number of 'Articles', protect the rights of citizens. Some of these Articles are absolute whereas others are 'qualified' and any interference with these is limited.

Interference with qualified rights is permissible only if:

There is a clear legal basis for the interference with the qualified right that people can find out and understand, AND

The Action/Interference seeks to achieve a legitimate aim.

Legitimate aims are set out in each article containing a qualified right and they vary from article to article.

This includes for example, the interests of National Security, the prevention of disorder or crime and public safety. Any interference with one of the rights contained in articles 8 -11 must fall under one of the permitted aims set out in the relevant article.

The action is necessary in a democratic society. This means that the action or interference must be in response to a pressing social need and should be assessed by demonstrating evidence of a level of severity or immediacy/unpredictability, and alternatives should have been reviewed.

The use of BWV must comply with the all the Articles of the HRA, and there are two particular Articles that are critical and most likely to be challenged. Article 8 of the ECHR is the right to respect for private and family life, home and correspondence. Under the legislation, this article is a qualified right and, there is requirement to consider this article when dealing with recorded images, whether they are made in public or private areas.

Accordingly, this assessment looks to address the issues raised by this Article and introduces suitable safeguards, associated with how DAERA Inland Fisheries deploys this equipment, in both the public and private arenas, and then how it deals with the products from any use.

Throughout, the principle objective is ensuring that any interference with the rights of parties can only be justified if it is:

- o **Necessary**

- o **In pursuit of a legitimate aim** – such as the prevention, investigation and detection of crime, with the necessity test being satisfied by the presence of a pressing social need.

- o **In accordance with the law**

Article 6 of the ECHR provides for the right to a fair trial.

All images from BWV have the potential for use in court proceedings whether they provide information that is beneficial to the prosecution or defence. The information will be safeguarded by an audit trail in the same way as other evidence that is retained for court.

It must be emphasised that BWV can collect valuable evidence for use in criminal prosecutions, ensure fishery officers act with integrity and transparency and potentially provides objective evidence of controversial events.

Surveillance Processes Body Worn Video

It offers protection for both citizens and the police. However this justification may be closely scrutinised by a court and it is essential that BWV recordings will not be retained where there is no clear evidence of an offence, unless some other good reason exists for their retention.

Recordings of persons in a public place are only public for those present at the time, so those situations are therefore still regarded as potentially private

Recorded conversations between members of the public should always be considered private.

Users of BWV must consider Article 8 when recording and must not record beyond what is necessary for regulatory purposes.

DAERA Inland Fisheries has imposed stricter guidelines where BWV is being used in places not open to the public or where a person being recorded would have a strong expectation of privacy. These include:

Legal privilege

Users will respect legal privilege and must not record material that is, or is likely to be, subject to such protections.

Journalistic Material

This equipment will not be used in any way in which it is likely to collect journalistic material.

Expectation of Privacy

Individuals are likely to have a strong expectation of privacy, in places not generally open to the public, such as a private residence. Clear justification of the necessity to use BWV will be required in such circumstances. Furthermore circumstances may dictate an expectation of privacy.

Formal interviews

BWV should not be used for formal investigative interviews, e.g. the Achieving Best Evidence interview for evidence in- chief purposes, or a significant witness interview for the purpose of preparing a statement. The use of BWV for the formal interview of suspects is not permitted as it would be in contravention of **PACE Code C** and it is currently unsuitable for recording interviews with vulnerable or intimidated witnesses. BWV should only be used in such circumstances where it is strictly necessary in order to gather evidence and/or moderate behaviour, and there is no other reasonable means of gathering the necessary evidence.

It is fully acknowledged that there will be some circumstances where the use of BWV, especially within a private place, is likely to raise special concerns over privacy.

Officers have to demonstrate in such circumstances that they are addressing a 'pressing social need' by using the equipment since this is 'an interference' under the legislation.

This could include incidents and investigations into reports which may involve the risk of violence or abuse against officers within a private environment, but even then, devices should only be used when alternative means of obtaining the necessary quality and conclusive standard of evidence, have been considered and discounted. In these instances, particularly where officers enter a private place, the use of BWV

Surveillance Processes Body Worn Video

can provide compelling and corroborative evidence which ordinarily cannot always be adequately conveyed through solely written statements. It is therefore complementary in that it is capable of providing the best possible evidence to capture any comments, demeanour and overall appreciation of the scene.

Surveillance Processes Body Worn Video

Data Protection Act 1998

The Data Protection Act 1998 (DPA) is legislation that regulates the processing of personal data including sensitive personal data, whether processed on a computer, CCTV, stills camera or any other media. Any recorded image and audio recording from any device, which includes BWV, that can identify a particular person or learning about their activities, is described as personal data and is covered by the DPA and in particular by the principles contained within it. Principle 1 of the DPA (fair and lawful processing) requires that the data subject must be informed of:

1. The identity of the data controller
2. The purpose or purposes for which the material is intended to be processed and
3. Any further information that is necessary for processing to be fair

DAERA Inland Fisheries has the responsibility for controlling this information and is known as the Data Controller for information captured and used within its area, for a regulatory purpose. If required, an officer using a BWV device must be prepared to explain how the capture and processing of any data is compliant with the legal obligations imposed under this Act.

DAERA Inland Fisheries have provided BWV devices to Officers which have incorporated front facing illuminated display screens coupled with a visible red light when in operation to reinforce the overt nature of any recording, this will be accompanied by clear verbal instruction that a situation is being recorded. Therefore this condition is considered to have been satisfied.

BWV devices must not be used in any covert capacity

The sharing of BWV images with other agencies and the media, will only occur in accordance with the requirements of the Act.

Criminal Procedure and Investigations Act 1996

The Criminal Procedure and Investigations Act 1996 introduced the statutory test for disclosure of material to the defence in criminal cases.

DAERA Inland Fisheries is able to disclose both used and un-used images and demonstrate that this has been done. Deletion of any generated images (or a third party's images in DAERA possession) prior to their respective retention periods, may amount to a breach of the Act if they are not then available for disclosure. Images that are relevant to an investigation must be retained in accordance with the Code of Practice issued under Section 23 of the CPIA.

DAERA generated digital images should be accompanied by a full audit trail, from the point of capture of the image throughout the whole management process – including when they are passed to the Prosecution or the defence or if there is any supervised viewing.

Freedom of Information Act 2000

The Freedom of Information Act 2000 grants a general right of access to all types of recorded information held by public authorities, which includes digital images recorded by BWV.

The Act does however provide some specific exemptions to the requirements to disclose information.

Data Flows

Surveillance Processes Body Worn Video

DAERA Inland Fisheries has the responsibility for the processing of information in its possession which commences at the point when an officer captures it. Clearly, when information is identified as being non-evidential, this follows a process whereby it is automatically deleted after a short determined timeframe. In circumstances where the information is evidential, master and working copies are created and retained. At the conclusion of any investigation, there is a requirement to hold the data strictly in accordance with requirements which detail specific time frames based on the nature of the offence/incident, and includes undertaking appropriate reviews, further retentions if appropriate and then disposal.

Privacy Issues and Risk Mitigation

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

BWV is a relatively new technology being deployed by DAERA. DAERA recognises the potential concerns from the public regarding privacy issues. Accordingly, this technology will only be deployed in an overt manner, using trained staff and in defined operational circumstances. All captured data will be processed, retained if relevant and subsequently disposed of in accordance with the Data Protection Act and Human Rights Act 1998.

When capturing information on these devices, officers will only do so in order to fulfil a regulatory purpose. The legitimate regulatory purpose behind the use of this equipment is to prevent and detect fisheries offences and prevent public disorder in association with fisheries offences. When information is captured, it will firstly be assessed as to whether it constitutes evidential or non-evidential material. Any material, which is deemed as evidential, could then be shared with DAERA Prosecution Service, Defence professionals and the Courts to support a prosecution. Any sharing of the information outside these parameters will generally not be permitted.

Any captured information deemed to be evidential, will in the first instance be 'protected' by means of a Master copy being created. This remains an integral part of the process. A Working copy(s) is created and it is this which will be passed to other Criminal Justice partners, the Defence and ultimately the Court. In instances of any dispute, the Court can require the production of the Master copy.

DAERA will only deploy this technology against the defined operational requirements and to ensure that the use is proportionate, legitimate, necessary and justifiable. In addition, it will ensure that the use satisfies the requirement of addressing a pressing social need. At all stages it will comply with the Data Protection Act and other legislation. In the case of the Human Rights Act 1998, there will be adherence to the requirements of Article 6 (Right to a fair trial) and in respect of Article 8 (Right to respect for private and family life, home and correspondence) since this is a qualified

Surveillance Processes Body Worn Video

right, information will only be captured and processed to achieve a legitimate aim as detailed earlier.

BWV technology allows the capture of both video and audio data which differs from CCTV but a principle issue is that without the introduction and adherence to essential safeguards, there is the greater risk of the possibility of widespread intrusions into the privacy of the public. However there are appropriate policies and legislative requirement imposed on its use, which will minimise this risk.

It is widely recognised that members of the public are likely to have a strong expectations of privacy especially in their own homes. Indeed this is contained with Article 8 of the ECHR (a right to respect for a private and family life) and under normal circumstances BWV should not be used in private dwellings.

However if a fishery officer is present at an incident in a private location and is there for a 'genuine regulatory purpose' and this equipment is able to address a 'pressing social need' then the officer can consider making a BWV recording in the same way in which any other incident is recorded.

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

In circumstances where an occupant or owner of a premises objects to the recording but where an incident is taking place, involving risk, threats or intimidation of investigating officers or allegations of a criminal nature are being made, officers are recommended to continue with a recording but explain their reasons for doing so. There is a clear requirement to secure the best evidence of any offences that have occurred and that the video/audio evidence will be more accurate and of a higher quality and therefore in the interests of all parties

That continuing to record would safeguard both parties, with a true and accurate recording of any significant statements made by either party and of the scene in general

Continuing to record will safeguard the BWV user against any potential allegations from either party. DAERA is mindful of the concerns that this raises and will train users to respect and adhere to these safeguards