Cambridge City Council

Body Worn CCTV Camera

Operational Procedure

Adopted: **1 August 2016**

Reviewed:

1. Introduction

1.1 This document sets out the Council's Policy and Procedural Guidelines for the use of Body worn CCTV cameras (BWC) by Council authorised Enforcement Officers (EO). It will enable EO's to comply with the relevant legislation relating to video recording and outline the associated benefits to EO's and the general public. It also documents best practice procedures with regard to legislation, integrity of data, images and video as well as its security and use.

1.2 The use of BWC can provide a number of benefits which include a deterrent to acts of aggression or verbal and physical abuse toward EO' s and the provision of evidence to support Police investigations, complaints made by the public and disciplinary investigations.

1.3 BWC forms part of an EO's Personal Protective Equipment and is provided solely for the use indicated in the Code of Practice. It will be used in an overt manner and emphasised by the wearing clear identification that it is a CCTV device. Prior to commencement of any recording, where possible, EO's will give a clear verbal warning / hand signal that recording is taking place.

1.4 The EO uses of BWC (and what they will not be used for) are set out in the accompanying Code of Practice to this document.

2. Legislation

2.1 The integrity of any video data recorded will be considered in accordance with the legislation, policies, procedures and guide lines set out in the Code of Practice. Notes on the legislation relating to the use of BWC as a form of CCTV are at Annex 'A'.

3. On Street Operational Guidance and Best Practice

3.1 Training

All EO's will receive full training in the use of BWC. This training will include practical use of equipment, on street operational guidance and best practice; when to commence and cease recording; and the legal implications of using such equipment. Records of EO's training will be stored on the EO's training record and refresher training will be provided annually. EO's will not be deployed with BWC until training has been undertaken.

3.2 Daily Use

Recordings will not commence until the EO has issued a verbal warning (if practical see Code of Practice), of their intention to turn on the BWC. The exception for circumstances where staff would not issue a warning is mentioned in section 1.3

Recordings will not be made whilst performing normal patrolling duties.

All recordings will be held securely.

Access to recordings will be restricted to authorised personnel as indicated in the Code of Practice, Legal Services and HR.

The responsibility for the security of the BWC rests with the Head of Service or Responsible Officer. If the BWC is lost, stolen or damaged it MUST be reported immediately to the Head of Service so an investigation can be mounted to minimise damage especially regarding the loss of any personal Data.

3.3 Start of Shift Procedure

All EO's will be issued with their own BWC device. At the commencement of each shift the EO will ensure that the unit is fully functioning. It will be the EO's responsibility to advise the Responsible Officer of any malfunction with the BWC. The check will also include verifying that the unit is fully charged and that the date and time displayed is correct by comparing it to the office based PC`S.

3.4 Recording

Recording must be incident specific. EO's must not indiscriminately record entire duties or patrols and must only use recording to capture video and audio of specific incidents. For the purposes of this guidance an 'incident' is defined as:

a) An engagement with a member of the public which in the opinion of the EO is confrontational, and where the EO believes they may be subject to physical or verbal abuse.

b) The EO is approached by a member of the public in a manner perceived as aggressive or threatening.

c) EO witnessing a littering, fly tipping, dog fouling, Punt Touting or other form of Environmental Crime (e.g graffiti or illegal advertising) offences.

At the commencement of any recording the EO should, where possible, make a verbal announcement to indicate why recording has been activated.

The purpose of issuing a verbal warning is to allow a member of the public to modify any unacceptable confrontational or aggressive and threatening behaviour. If, at any time during an incident the EO considers that the use of the BWC or the issuing of a verbal warning, is likely to inflame a confrontational situation, the EO may use discretion to disengage from further discussion and withdraw from the incident.

A specific form of words to be used in any warning to a member of the public has not been prescribed, but an EO should use straightforward speech that can be easily understood by those present, such as:

'I am wearing a Bodyworn Camera and I am now recording '

3.5 Playback

EO's will need to be fully aware of the legal implications once digital images and audio have been recorded. To this end playback should only be at the request of an officer listed in the Code of Practice subsequently involved in the investigation of the incident. Any request to view captured video by a member of the public, will need to be made in writing to Cambridge City Council in line with the Data Protection Act's 'subject access procedure'. Evidence of identity prior to viewing must also be provided. Note access to images by the public will not be permitted in certain circumstances, see Annex 'A'.

3.6 End of Shift

EO's should ensure that any BWC footage required for evidential purposes has been correctly bookmarked and that any system records and pocket note book entries have been completed.

EO's will be responsible for ensuring all BWC have been connected correctly to the docking station to enable downloading and charging.

3.7 Storage of Data

All recorded footage will be uploaded to a secure Cambridge City Council IT system by the EO on duty in an office with restricted access.

EO's will ensure that any footage to be retained has been correctly bookmarked and that system records have been completed.

For incidents where the EO thinks a referral to another enforcement agency is necessary the Responsible Officer will review the recording and, in consultation with the EO operating the device, a decision will be made on whether referral is appropriate.

The EO will then transfer the data from the secure Cambridge City Council IT system on to a secure encrypted external hard drive and complete the Information Asset Log.

All retained data will be kept until all investigations have been completed or a prosecution has taken place. If no action is taken, recorded footage should be destroyed after 31 days.

Any other data, not required for evidential purposes, will be deleted by the EO by the next working day, Monday to Friday.

3.8 Authorised Officer's:

Head of Environmental Services.

Senior Operations Manager, Streets and Open Spaces.

Operations Manager (Community Engagement and Enforcement), Streets and Open Spaces (Responsible Officer).

Public Realm Enforcement Officers and the Dog Warden Service (EO's / Authorised Officer).

Police and other Enforcement Agencies.

Authorised Investigating Officers, HR and Legal if required.

Signed by:

Name:

Appointment:

Date:

Distribution:

Annex 'A': Notes on Legislation

Annex 'A' to Operational Procedures For Cambridge City Councils Body Warn Cameras (BWC). Dated April 2016

Notes on Legislation affecting CCTV Operations

Reviewed July 2016.

1. There have been a number of Acts passed by Parliament, which will affect the way that CCTV systems are operated. In particular the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 and Acts relevant to other agencies.

1.1 This Annex is not an authority on these Acts but rather gives a general introduction to each of the relevant Acts and provides some guideline as to how CCTV systems should be operated to ensure they comply with the legislation. Detailed advice on the legislation should be sought from the Head of Legal Services.

1.2 **Local Authority use of RIPA.** It is important that all Council staff are aware that changes were made to Local Authorities use of RIPA. The basic rule is that RIPA may not be used by the Authority unless the offence is likely to carry a custodial sentence of 6 months or more and is approved by a Magistrate. Any consideration of a Council instigated RIPA operation **MUST** be discussed with the head of Legal Services before any action is taken. The Council's policy on use of RIPA is available on the Intranet.

2. The Data Protection Act 1998 (DPA)

2.1 The Act relates to data processing of all types. CCTV images recorded by CCTV cameras fall within the Act. As a result our CCTV systems have been registered with the Information Commissioner.

2.2 Cambridge City Council's BWC's will be clearly marked with a sign that is of a suitable size so that people can easily read it. The sign is there to inform people that a BWC is being worn and is operational.

2.3 The Information Commissioner has set out eight principles to ensure that CCTV systems meet the requirements of the DPA. These are:

- All personal data will be obtained and processed fairly and lawfully.

- Personal data will be held only for the purposes specified.
- Personal data will be used only for the purposes, and disclosed only to the people, shown within the Council's Code of Practice and Operational Manual.
- Only personal data will be held which are adequate, relevant and not excessive in relation to which the data is held.
- Steps will be taken to ensure that personal data are accurate and where necessary, kept up to date.
- Personal data will be held for no longer than is necessary.
- Individuals will be allowed access to the information held about them and, where appropriate, permitted to correct or erase it.
- Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information.

2.4 To ensure compliance with the Data Protection Act, Cambridge City Council's CCTV systems are subject to the Council's Policy Statement, Code of Practice and systems Operational Manuals to ensure that the following rules are observed:

- All recorded images will be of good quality and factually correct.
- All discs/ tapes will be marked with a unique serial number.
- Only authorised personnel will be permitted to view images.
- Only trained and authorised Council staff will be permitted to operate the CCTV equipment.
- Browsing of images for potential incidents will not be permitted.
- The investigating officer will be required to sign for any images removed from the CCTV system so that a clear audit trail of evidence is maintained.
- All images recorded on the CCTV system and not required for investigation will be destroyed or over written approximately 31 days after recording.
- Images may be retained longer than 31 days but only at the request of an enforcement agency or Investigating Officer to continue an investigation.

- All recording media will be kept secured at all times.
- The Responsible Officer will be responsible for the security of the images held in each location.
- The location of all recording media must be known at all times.
- Recording quality will be audited monthly.
- All images recorded by the CCTV cameras will have the date, time and the location of the camera providing the images clearly superimposed on them.
- All equipment within the CCTV system including cameras, recorders and monitors will be checked regularly and faults reported and repaired as quickly as possible.
- Authorised staff will not view private areas except under the conditions set out in section **4** of this Annex.
- Staff will only monitor individuals whom they believe have committed or are about to commit an offence.
- Staff will not use the cameras to follow individuals because of their sex, colour, race, dress or appearance. Nor will they stereotype members of the public.
- No images of any kind produced by Cambridge City Council's CCTV systems will be released for commercial or entertainment purposes.
- No recordings or still images will be produced for any other purpose than the achievement of the aims and objectives set out in the systems Code of Practice.

2.5 A person may request a viewing of images they believe the BWC CCTV system has of them or a copy of the images by contacting Cambridge City Council's Information and Data Policy Officer on **01223-457062**. They will then be supplied with a Data Access Request Form, which must be filled in, in all parts, and returned to the Information Management Officer.

2.6 The Responsible Officer on receipt of the request will isolate the relevantimage and, providing the following criteria are met, will comply with the request within forty days. The criteria are:

- The application form has been fully completed.
- Information is provided to confirm details of the individual.

- Sufficient information has been supplied to locate the relevant recording i.e. date, time, location, description of individual and their activity.

- The necessary administrative fee has been paid.

- The written request is received within 28 days of the image being recorded.

2.7 The Responsible Officer may not comply with the request in the following circumstances:

- If images of third parties are also in the frame and their permission for disclosure cannot be obtained.

- If the request is considered to be unreasonable or vexatious.

- If the images are in connection with a potential crime and evidence of an incident may be investigated or is under investigation by an enforcement agency or an internal investigation. The responsibility for disclosure in cases involving enforcement agencies rests with them and not with Cambridge City Council.

3. The Human Rights Act 1998 (HRA)

3.1 The Human Rights Act into force in 2000. The Act gives "further effect to the rights and freedoms guaranteed under the European Convention on Human Rights".

3.2 The HRA does not bring any new rights or criminal offences, but the Act does bring existing rights into force as part of UK domestic law, which will enable people in the UK to have cases dealt with in UK courts rather than having to take them to Europe for a ruling as was the case before this Act was passed. The Act also gives public authorities (Cambridge City Council) a legal duty to act compatibly with the Convention rights.

3.3 Some of the rights under this Act are 'Qualified rights'. These are rights that may be interfered with or restricted by the state if the activity threatens national security, public safety or health or to deter or detect crime etc. However these rights can only be restricted if the need for that restriction can be shown to be **P**roportionate, **L**egal, **A**ppropriate and is **N**ecessary (**PLAN**).

3.4 The Responsible Officer is responsible for ensuring that the BWC CCTV system does not infringe individual's rights under the HRA. They along with other Cambridge City Council Managers will be responsible for challenging any infringements it is being asked to assist in imposing by other agencies (through surveillance under RIPA, see section **4** below), by

challenging any request it receives and by applying PLAN to any such restriction and obtaining satisfactory justifications to any such requests.

3.5 The Articles, which will have a direct impact on the operation of Cambridge City Council's BWC CCTV systems, are:

a. **Article 6: RIGHT TO A FAIR TRIAL**. When gathering, processing and producing evidence it must be done so legally in line with the DPA and the HRA. EO's must bear in mind that the evidence being produced can be used to prove innocence as well as guilt. Although it is an Enforcement Agencies responsibility for disclosure of evidence. EO's must ensure that other enforcement agencies are made aware of all the cameras used whilst monitoring an incident. It is for the enforcement agencies to decide what is or is not relevant evidence and not the EO.

EO's must ensure that all details concerning the production and issue of any evidence captured by BWC's are accurately recorded.

b. **Article 8: RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE**. It is recognised that everyone has the right to respect for their private and family life, their home and their correspondence. Except for the prevention of disorder or crime and for the protection of the rights and freedoms of others. Cambridge City Council's BWC system has been set up with clearly defined objectives, which are shown in full in the Cambridge City Council's BWC Policy Document and in individual systems Codes of Practice**.**

The systems clearly recognises people's 'right to privacy' by ensuring all its Operators are properly trained, that there are clear guidelines in the BWC Operational Manuals and Codes of Practice and that regular audits of the system are carried out.

Although general observations will be maintained EO's operating BWC's will not follow individual members of staff or the public except when an offence has been committed or in the judgment of the Operator is about to be committed.

Any images captured by BWC's will be held for a maximum of 31 days and then destroyed except when an investigating officer requires the evidence to be retained for investigation or prosecution. No BWC images will be released for commercial or entertainment purposes.

c. **Article 10: FREEDOM OF EXPRESSION**. This article carries with it duties and responsibilities by the people who wish to exercise these freedoms. Therefore EO's operating BWC's will only monitor such events in the interest of public safety, the prevention of disorder or crime, to protect the rights of others and to assist in enforcing any lawful restrictions placed on any such activity.

d. **<u>Article 11: FREEDOM OF ASSEMBLY AND ASSOCIATION</u>**. Everyone has the right to peaceful assembly and freedom of association. EO's will only monitor these events in the interest of public safety, the prevention of disorder or crime, the protection of the rights and freedoms of others and to assist in enforcing the lawful restrictions placed on any such event.

e. **<u>Article 14: PROHIBITION OF DISCRIMINATION</u>**. Cambridge City Council has very clear policies on discrimination. All EO's must be aware of the Council's polices. In addition, all EO's will attend extra anti-discrimination training. No EO will monitor an individual because of their sex, race, colour, dress, appearance or monitor individuals by stereo typing them in any way.

3.6 All EO's must understand that they have a clear responsibility as the operators of the system to assist Cambridge City Council in its duty to uphold the HRA. EO's should do nothing that is likely to breach the HRA. If any EO's find themselves in a position were they are unclear as to how they should respond, they are to contact the systems Responsible Officer, the Council's CCTV Manager or the Legal Services for guidance.

4. <u>The Regulation of Investigatory Powers Act 2000 (RIPA)</u>

4.1 This section should be read in conjunction with the **Procedure guide to the use of covert surveillance and 'covert human intelligence sources' Jan 2015**, which is on the Council's Intranet Site.

4.2 The Regulation of Investigatory Powers Act received Royal Assent in July 2000. The aim of the Act is to ensure that the investigatory powers of the intelligence service, police and the military, local authorities and others are used in accordance with human rights. The Act provides a basis for authorisation and use by organisations of 'surveillance' (including BWC) and regulates the techniques employed and safeguards the public from invasions of privacy.

4.3 This Act can be used for surveillance in the following categories:

a. In the interests of national security.

b. To prevent or detect crime or prevent disorder.

c. For the economic well-being of the United Kingdom.

d. In the interest of public safety.

e. For the purpose protecting public health.

f. Assessing or collecting of any tax, duty or levy.

g. For any other purpose ordered by the Secretary of State.

h. For Local Authorities: For the purpose of preventing or detecting serious crime where the offence under investigation carries a custodial sentence of six months or more.

4.4 The Act does not cover the use of overt BWC systems, as staff and members of the public are aware that such systems exist and are a means of detecting and deterring crime. Using BWC for evidence gathering in the event of an offence do not need to be authorised under RIPA. However, pre-planned, covert operations to follow known individuals, target premises or specific vehicles, which involve the use of BWC, may need authorisation.

4.5 The Act deals with 'covert surveillance', which is defined as: "Observations, which are carried out by, or with, surveillance devices". Surveillance will be covert where it is carried out in a manner calculated to ensure that the person or persons subject to the surveillance are unaware that it is, or may be, taking place. Covert surveillance is divided into two types, 'direct' and 'intrusive'

a. **Direct Surveillance** is covert but not intrusive and is undertaken:

(i). For a specific investigation or a specific operation;

(ii). In such a manner as is likely to result in obtaining private information about a person; and

(iii). Otherwise than by way of an immediate response to events or circumstances, which would not allow time for authorisation to be obtained under this section (26) to carry out surveillance.

b. **Intrusive Surveillance** which is not carried out by Cambridge City Council's BWC system, is covert surveillance that:

(i). Is carried out in any residential premises or any private vehicle and;

(ii). Involves the presence of an individual or a surveillance device on the premises or in the vehicle.

4.6 No 'covert' operation will be undertaken by Cambridge City Council's BWC systems unless an authorisation form specifying the use of the BWC system is produced by the relevant agency requesting assistance to enable CCTV to assess its involvement in the operation and gather details for its records which should include details of:

- the serial number and operation code name;

- the name and rank/position of the authorising officer and their contact details;
- the start date and duration of the operation. Finish date and any extensions to the operation;
- the target of the operation and;
- what the EO's BWC systems involvement will be in the operation.

4.7 All requests for pre-planned surveillance operations are to be directed to the systems Responsible Officer who will then follow the procedures set out in paragraph 4.1. In the event of the Responsible Officer being absent, the request should be passed to the Head of Service or Director for permission for the CCTV system to be used in the operation.

4.8 Authorising Officers from the police will normally be a Superintendent or above and they may authorise operations for up to three months. In an emergency, an Inspector may authorise the surveillance request but the operation may only last for seventy-two hours unless written counter-authoris ation is received from a Superintendent or above.

4.9 Authorising Officers from the City Council are identified in the document in paragraph 3.8 above and other organisations will be at the level stipulated in the Act.

4.10 All City Council staff should be alert to so called experts from other agencies claiming that an operation does not require RIPA authorisation. The trigger for your concern should be any pre-planned operation involving identified individuals, vehicles or buildings. Staff must not allow themselves to be bounced buy these experts but discuss the issue with the Head of Legal Services.

4.11 To enable officers to assess under PLAN whether they should assist in a RIPA operation, they must be given sufficient information about the operation by the requesting authority. In the Surveillance Commissioner's view if that authority claims that the information is too sensitive to share, then BWC is probably not the right way to mount the operation and the request should be refused.

5. The Freedom of Information Act 2000 (FOIA)

5.1 The Freedom of Information Act (FOI) was passed in 2000 and was Fully implemented in 2005. The Act provides a general right of access to all recorded information (including BWC images) held by public bodies without significant formality or inquiry into the motives of the applicant and at subsidised cost.

5.2 Rights granted under the Act provides that any person making a

request for information to a public authority is entitled to be informed in writing by the public authority whether it holds information of the description specified in the request and if that is the case, to have that information communicated to them.

5.3 Under the Act the definition of 'information' means information recorded in any form and is fully retrospective. It includes personal and non-personal information.

5.4 Under the FOI Act it is a criminal offence to alter, deface, erase, destroy or conceal any record held by the council, with the intention of preventing the disclosure of all, or part, of the information to which the applicant would have been entitled.

5.5 Applications for information may come from individuals or legal entities such as a company. Applicants do not have to mention any Acts nor do they have to give a reason for their application when applying for information but requests for information must be in writing in the form of an Access Request Application Form. If the request involves images of third parties, this will amount to 'Personal Data' and must be dealt with under the DPA.

5.6 The FOI Act should not unduly affect EO's using BWC. Their current dealings with and passage of information between partners will continue. However any requests for information from applicants outside these partnerships should not be dealt with by EO's using BWC but must be passed onto the City Council's Performance Analyst who has responsibility for dealing with Access Request Applications.

5.7 If an applicant is not satisfied with the way their application has been dealt with, they may make a complaint using the Council's complaints procedure or they may contact the Information Commissioner direct.

6. The Protection of Freedoms Act 2012.

6.1 The Protection of Freedoms Act was introduced to further protect people's rights and to further protect them from intrusion by public bodies.

6.2 The Surveillance Camera Commissioners Code of Practice (COP) provides guidance in the use of Surveillance (CCTV) Cameras and Automatic Number Plate Recognition Cameras (ANPR) but does not replace statutory obligations on operators or users set out in other existing legislation.

6.3 The Act covers the use of surveillance cameras by 'Relevant Authorities' such as Cambridge City Council but does not cover privately owned or operated CCTV systems (retail, home or other users) but those owners are encouraged to adopt the **Guiding Principles** set out below in the interests of '**Best Practice**'.

6.4 The Surveillance Camera Commissioners has set out **12 Guiding Principles** to be adopted by operators and users to help them comply with the Act. These principles are:

1. Use of Surveillance camera systems must always be for a specific 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 surveillance camera systems 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 collection, 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 its purpose has been discharged.

7. Access to retained images and information should be restricted and here 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 the system and its purpose and work to meet and maintain those standards.

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

10. There should be effective reviews 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 a pressing need, 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 matches against a reference database for matching purposes should be accurate and kept up to date.

6.5 A more detailed explanation of each of the **Guiding Principles** (above) is shown in the Surveillance Camera Commissioner's COP which is available in full on the CCTV website along with a **Privacy Impact Assessment Book**. It is recommended that all those responsible for CCTV systems read these documents and the **Information Commissioners COP**, which is also available on this site.