Woking Borough Council Parking Services

Body Camera Code of Practice v.1

Contents

Operational Procedural Guidelines

Introduction

This document sets out Woking Borough Council's Procedural Guidelines for the use of Body-worn cameras (BWC) by Civil Enforcement Officers and Car Park Attendants (CEO's/CPA's) who patrol the borough.

It will enable employees to comply with relevant legislation relating to video recording and outline the associated benefits to CEO's/CPA'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.

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

BWC form part of a CEO's/CPA's Personal Protective Equipment and is provided solely for Health and Safety purposes. It will be used in an overt manner and emphasised by CEO's/CPA's wearing clear identification that it is a CCTV device.

CEO's/CPA's start recording once they have reason to believe that they are in, or about to be in a confrontational situation, where possible, they will give a clear verbal instruction that recording is taking place.

BWC will not be used to gather evidence for traffic enforcement purposes nor will it be used as a tool to assist in the ad-hoc monitoring of staff.

1. Legislation & Statutory Guidance

The integrity of any video data recorded will be considered in accordance with the following legislation and Statutory Guidance:

Data Protection Act 1998

Freedom of Information Act 2000

Human Rights Act 1998

Protection of Freedoms Act 2012

Home Office Surveillance Camera Code of Practice Information Commissioners Code of Practice

1.1 Data Protection Act 1998

The Information Commissioner's Office is the regulator for the Act and has given guidance with regard to CEO use of BWC equipment. This legislation regulates the processing of 'personal data' or 'sensitive personal data' whether processed on computer, CCTV, still camera or any other media.

Any recorded image that is aimed at or may identify a particular person is described as 'personal data' and covered by this Act and will include images and audio captured using BWC equipment. The use of BWC in this guidance is 'overt use' meaning that equipment is not to be worn or used in a hidden or covert manner.

Where an individual asks to view footage this is called a 'Subject Access Request'. The requester is only allowed to see footage of themselves and anyone who has provided consent for their images to be viewed by them. It should be noted that there may be circumstances in which the footage will not be released.

1.2 Freedom of Information Act 2000

This Act grants a general right of access to information held by public bodies, which is not personal data. Information released under Freedom of Information (FOI) can include statistical and other non-personal information.

1.3 Human Rights Act 1998

Article 6 provides for the right to a fair trial. All images captured through the use of a BWC device have the potential for use in court proceedings and must be safeguarded by an audit

trail in the same way as any other evidence.

Article 8 of the Human Rights Act 1998 concerns the right for private and family life, home and correspondence. Recordings of persons in a public place are only public for those present at the time and can still be regarded as potentially private. Any recorded conversation between members of the public should always be considered private and users of BWC equipment should not record beyond what is necessary when recording a potentially confrontational situation.

Woking Borough Council will ensure that the use of BWC equipment by its CEO's/CPA's is emphasised by wearing it in a prominent position (normally on their chest) and that its forward-facing display is visible to anyone being recorded. Additionally, the BWC is a Pinnacle Response (PR5 or PR6) which clearly has the wording "CCTV" in large writing on the front of the device. The CEO's/CPA's will, where possible, make a verbal announcement at the commencement of any recording.

1.4 Protection of Freedoms Act 2012

Part 2 creates new regulation for, and instructs the Secretary of State to prepare a code of practice towards, closed-circuit television and automatic number plate recognition.
Chapter 1 gives the full regulatory legislation of CCTV and other surveillance camera technology which relates to a Code of Practice and interpretations.

1.5 Home Office Surveillance Camera Code of Practice

The integrity of any video data recorded will be considered in accordance with this Statutory Guidance.
The Home Office is the regulator for this guidance with regard to CEO's/CPA's use of BWC equipment. This guidance is centred around "12 Guiding Principles" which Woking Borough Council will adhere to at all times.

1.6 Information Commissioners Code of Practice

The Information Commissioners Code of Practice is the Statutory Guidance issued that runs in conjunction with the Surveillance Code of Practice issued with regard to CEO's/CPA's use of BWC equipment.

2. On Street Operational Guidance and Best Practice

2.1 Training

All CEO's/CPA'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. Additionally, CEO's/CPA's receive ongoing refresher training in 'Conflict Awareness'. CEO's/CPA's will not be deployed with BWC until training has been undertaken.

2.2 Daily Use

BWC will only be used in the event that a CEO/CPA has reason to believe they are in or about to be in a confrontational situation and/or they are subject to, or feel that they are likely to be subject to, verbal or physical abuse.

Recording will commence when the CEO/CPA has reason to believe they find themselves in a confrontational situation. Where possible, they will give a clear verbal instruction that recording is taking place.

Recordings will not be made whilst performing normal patrolling duties.

All recordings will be clearly archived in designated electronic folders and held on an encrypted hard drive or on the Cloud system, which can only be accessed using a password protected laptop. Access to recordings will be restricted to the Parking Services Management, Legal Services, HR and Compliance/Audit Manager.

2.3 Start of Shift Procedure

All CEO's will be issued with their own BWC device. CPA's will be issued with a Body-worn device when going on patrol. At the commencement of each shift/Patrol the CEO/CPA will ensure that the unit is fully functioning and that it has been cleared of all previous recordings.

The check will also include verifying that the unit is fully charged and that the date and time displayed is correct.

2.4 Recording

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

An engagement with a member of the public which, in the opinion of the CEO/CPA, is

confrontational or about to be confrontational or where the CEO/CPA believes that they may be subject to physical or verbal abuse or the CEO/CPA is approached by a member of the public in a manner perceived by the CEO/CPA as aggressive or threatening.

At the commencement of any recording the CEO/CPA should, where practicable, confirm their position as a CEO/CPA and 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 what would otherwise be regarded as unacceptable confrontational or aggressive and threatening behaviour. If, at any time during an incident the CEO/CPA considers that the use of BWC is likely to inflame a confrontational situation the CEO/CPA may use discretion to disengage from further discussion and withdraw from the incident.

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

"Sir / Madam, I would like to inform you that I am wearing a Bodyworn Camera and I am now recording this conversation"

2.5 Playback

CEO's/CPA's will need to be fully aware of the legal implications once digital images and audio have been recorded. The Pinnacle Response BWC is a closed unit and does not have the option to play the footage back to an offender or a Police Officer attending the incident.

Any request to view captured video by a member of the public will need to be made in writing to Woking Borough Council in line with the Data Protection Act's 'Subject Access Procedure'. Evidence of identity prior to viewing must also be provided.

2.6 End of Shift

CEO's/CPA's should ensure that all incident reports must be fully compiled. It will be the CEO's/CPA's responsibility to ensure that their BWC device is placed on charge at the end of their shift/patrol.

2.7 Storage of Data

All recorded footage will be downloaded to the encrypted hard drive by the parking services manager.

For Incidents where the Police have not been in attendance, The Parking Services Manager will review the recording and a decision made on whether referral to the Police is appropriate.

The Parking Services Manager will then transfer the data to a secure folder within the encrypted hard drive and name the footage as an exhibit using the initials of the officer and the number of the exhibit, as example JD/01.

All retained data will be kept until all investigations have been completed or prosecution has taken place before deletion. Once the case has been closed the footage will be deleted after 31 days. All data not required for evidential purposes will be deleted after download as part of standard operating procedures.

2.8 Transfer of data

Any footage requested by the police as part of their investigation will be encrypted and transferred to disc, labelled as an official exhibit and handed to them. Once in their possession the disc will fall under the police policy and guidelines for Data Protection.

Home Office Surveillance Camera Code of Practice

12 Guiding Principles

1. Introduction

1.1 This document sets out Woking Borough Council's response and clarification of compliance and conformity to the Home Office Surveillance Camera Code of Practice.

The document is our main referral document and Woking Borough Council endeavours to comply and conform to all guidance within the document but specifically, in this case, refer to the 'Twelve Guiding Principles'.

2. The 'Twelve Guiding Principles'

2.1 Use of a surveillance camera system must always be for a specified purpose which is in the pursuit of a legitimate aim and necessary to meet an identified pressing need.

See 'Operational Guidelines' pg. 3
See 'Your questions answered' – Questions 1 and 2

2.2 The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure it remains justified.

See 'Operational Guidelines' – pg. 3
See 'Your questions answered' – Questions 3, 4, 5 and 6

2.3 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 or complaints.

See 'Operational Guidelines' – pg. 3
See 'Your questions answered' – Question 7
See 'Privacy Impact Assessment' – Ref 7.3 See 'Press release and website information'

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

See 'Privacy Impact Assessment' – Ref 1.1, 1.2, 3.1, 3.5 and 3.8

2.5 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.

See Operational Guidelines' – pg. 3

2.6 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.

See 'Operational Guidelines' – pg. 3
See 'Your questions answered' – Question 6
See 'Privacy Impact Assessment' – Ref 7.1

2.7 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.

See 'Operational Guidelines' – pg. 3
See 'Privacy Impact Assessment' – Ref 3.1, 3.5 and 3.8

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

Woking Borough Council will be pro-active in keeping abreast with industry advancements and changes and make required adoptions accordingly.
Woking Borough Council will be looking to industry standard awards in the hope to obtain these.

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

See 'Operational Guidelines' – pg. 3
See 'Privacy Impact Assessment' – Ref 3.1, 3.5 and 3.8

2.10 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.

The asset manager will be responsible and accountable for the systems usage and this will be monitored and audited by the Enforcement Operations Manager and the Enforcement Team Leaders.
The cameras will be listed as an asset under the Health & Safety Personal Protective equipment list and the users will be referred to a disclaimer covering their responsibilities of all correct equipment usage. This will be extended to cover body cameras and the users will have to ensure that they will comply with the Operational Guidelines and any other training or guidance documents provided.

2.11 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 evidential value

See 'Operational Guidelines'
See 'Your questions answered'
See 'Privacy Impact Assessment'
See 'Press release and website information'

2.12 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.

The current 'HR34 & HR35 Incident Reports' form will be updated to include details of any footage captured by the body camera. These reports are logged and numbered internally and this number can be tagged onto the footage within the system software

Privacy Impact Assessment – Version 1.0 Woking Borough Council

This form is designed to help you carry out a high-level Privacy Impact Assessment (PIA). A PIA is a risk assessment for personal information, and is carried out as part of our compliance with the Data Protection Act and associated guidance from the Information Commissioner. The PIA will enable you to identify whether your project or system is likely to have an impact on the security of such information. The term 'system' includes any way of working – not just computer use – for example a manual filing system.

Using a PIA early in a project or system design will help to identify potential problems so that you can address them and take extra steps to protect information where needed. If after using this form there are indications of a significant impact on the way personal information is held and used, it may be necessary to do a more thorough assessment looking at each requirement of the Data Protection Act in detail.

You may not be able to complete the assessment in full early in the project, but you can update it later when the information is available. Where issues are identified, you should review the form later, for example before implementation, to ensure they have been addressed.

The Home Surveillance Commissioner has issued a Surveillance Camera Code of Practice which is our reference and we will be working with them to look at any areas of doubt and they will retain a copy of the completed assessment.

The camera hardware supplier is Pinnacle Response and we will be working with them to look at any areas of doubt and use their industry knowledge and experience.

Name of project: CEO's/CPA's Body-worn Camera
Department: Parking Services
Date form reviewed: 16th October 2017

Name of officer: Ian Reynolds (Parking Services Manager)
Date form completed: 16th October 2017
Name of officer: Ian Reynolds (Parking Services Manager)

Ref.	Question	Answer	Notes
1.1	Have you identified an Information Asset Owner, and if so, who is it?	Parking Services Manager	Each asset should be owned
1.2	Is the system being supplied and/or supported by a third party, and if so, how will their access to personal information in the system be controlled and monitored?	Yes, all Body Camera Footage is being held on an external hard drive, which is full encrypted and password protected. Once the footage has been downloaded to the hard drive, it is secured in a locked safe.	Companies who maintain systems may have to connect remotely in order to fix problems, apply upgrades etc.
1.3	If information will be processed by a third party, is there, or will there be, a contract in place?	In house	All processing will be done in-house.
1.4	If information will be processed by a third party, is there, or will there be, an agreement which defines how they will protect the information?	In house	Consider not only day-to-day processing but one-off requirements such as data scanning and conversion.
1.5	If a computer system is being hosted by a third party, is the data being held within the EEA or in a country where the arrangements have been assessed as being adequate?	Yes, hosted on an encrypted Hard Drive which is password protected.	Data Protection Act 1988, eighth principle. Data held outside the European Economic Area requires assessment.
1.6	If a system is replacing something else, what is happening to the old system or paper?	The external hard drive has not been replaced since contract commencement.	Secure archiving, storage or disposal may be required.

1.7	Does the system use identity management for citizens or other users, involving the authentication of the user through a token or other means? If so, have any concerns been fully investigated?	N/A	Automatic user recognition carries the potential for data loss through mistaken identification, and also for significant public concern over this. Consider too the security of original documents presented for identification purposes.
1.8	Does the system use new technologies of which the user may be suspicious, and if so, have sufficient time and resources been allocated to addressing this and allaying any concerns?	N/A	E.g. smart cards, RFID tags, biometrics, GPS and locators, image and video recording, and profiling. Technology which can be seen as intrusive generate public concern, and are a project risk.
2.1	If information will be held on paper (including prior to data entry) are the storage and disposal arrangements sufficiently secure?	Yes, HR34 and HR35 incident Reports.	Include consideration of office arrangements whilst documents are waiting or being processed.
2.2	If paper documents are being scanned into a system, is this done by the Post Room and then held securely? If not, has the risk of them being inadmissible in court been assessed?	N/A	If documents may be needed in court proceedings we must scan and hold them in a way which preserves their integrity to the court's satisfaction.
2.3	Will there be any adverse changes to the way records are handled, such as their version control, retention or	No	Future consideration required if changes are made.

	archiving?		
3.1	Is the system protected from unauthorised access through the council's network?	No, All footage is held and controlled within on an encrypted hard drive, which requires a password to be accessed.	Consider access hierarchy.
3.2	Is the system protected from unauthorised access through Internet?	Yes	The system cannot be accessed via the network or internet.
3.3	Is the system adequately protected from accidental loss of information (database, paper, backups etc.)?	Yes, all sensitive information obtained at the time of the offence is backed up.	Consider when backups are taken and how much work will need to be re-done in the event of a loss Consult Business Improvement and/or ITSD.
3.4	If the system can be accessed remotely, are measures to protect sensitive information adequate and do they meet the requirements of the IT Policy?	Not networked	Consider whether data can be transferred to remote computers i.e. Police or courts
3.5	How will you ensure that staff using the system are adequately trained in both the system itself and in information security, and that this training is kept up to date and refreshed?	Only the Parking Management Team will have access to system. All have received training in system use and data protection/security.	Consider both existing and new staff.
3.6	Are there sufficient controls over who can administer and use the system, and will administrators be suitably authorised and trained?	Yes	

3.7	If the system is accessible over wireless technology, are there sufficient controls to prevent access except from authorised devices?	N/A	Consider public Wi-Fi and personal devices, whether laptops or hand-held devices. Seek assurances from IT Service Delivery if required.
3.8	If the system uses a shared password are there adequate arrangements to change it frequently and after staff changes?	The password will be changed as soon as soon as staff leave.	We have a password which is shared between the Team Leader and Administrative Coordinator.
4.1	Will personal data be handled in a different way, that could mean it is linked to or matched with other data, requiring a review of how it is protected?	No	Data Protection Policy
4.2	Are you satisfied that Kingdom Security will be able to meet its obligations in respect of file access requests?	Yes	Subject Access Requests are part of the Data Protection Act 1998 (section 7)
4.3	Will the system attach a person's identity to information which would previously have been anonymous? If so has the potential for loss of privacy been investigated?	No	If data has previously been used in an anonymous way, any conversion to identifiable data will cause privacy concerns.
4.4	If the system holds sensitive personal data which merits special protection, have checks been made to ensure that this protection is present and consistent?	N/A	Section 2 of the DPA identifies categories of sensitive personal data including racial & ethnic origin, political opinions, religion, union membership,

			health, sexual life, offences and court proceedings.
4.5	If the system holds information about vulnerable people, have suitable measures been taken to protect that information?	N/A	The impact of the loss of information about vulnerable people is sufficient to warrant additional protection and checks.
5.1	If Woking Borough Council is not the Data Controller and Data Processor for the information, is it clearly agreed and documented who carries out these roles?	Yes, Woking Borough Council are the data processors and the data controllers and roles are laid down within this procedure.	See the Data Protection Act 1998.
5.2	If the system will use any data from other councils or organisations, are the necessary information sharing arrangements in place and documented?	N/A	May need considerations if a future partnership is set up.
5.3	If the data will be used in different parts of the council, are you satisfied that it is only being used for the purposes for which it was originally collected?	N/A	Data Protection Act 1998 – 2nd principle. Information sharing pages
5.4	Have arrangements been made for routine transfers of information to be carried out securely, and if so, how will this be done?	Any data for police use will be burned onto a hard disk and once handed to them will fall within the police data protection policy. No transfer of data to take place across a network.	Standard email and internet services between organisations must be regarded as insecure. Security covers loss, corruption and unauthorised access.

6.1	Have arrangements been made to assure the quality of the information being added to the system, both at take-on and daily?	N/A	Suitable measures can include validation routines, spelling checks, verification and sign-off of data.
6.2	Will processes be in place to ensure that there are no inconsistencies with data held in other systems, whether manual or otherwise?	N/A	It is good practice to hold data only once if possible, and access it as required.
7.1	Are you satisfied that the information held will still be accessible when required to answer Freedom of Information (FOI) requests?	Data will only be retained until investigations have taken place or prosecutions completed. All other data will be deleted.	Timely responses to requests are required by law (Freedom of Information Act 2000)
7.2	Have arrangements been made where appropriate to produce information for publication under Open Data requirements?	N/A	This information is published on the web site.
7.3	Will there be any changes to the publication scheme as a result of this project?	N/A	The publication scheme lists the information that we publish, or intend to publish, routinely. Doing this is a good way to avoid FOI requests.

This space is available to record any concerns arising from the assessment, and the action being taken to address them:

Ref.	Concern	Date	Action	Resolution	Date

BODY-WORN CCTV CAMERAS YOUR QUESTIONS ANSWERED

1. Why is Woking Borough Council providing BWC's to all of its CEO's/CPA's?

BWC's are being introduced as an improvement to the health and safety of our CEO's/CPA's. Since 2014 there have been several serious incidents whereby Woking Borough Council and the Police have been unable to take further action due a lack of evidence.

The use of these cameras will help to ensure that, wherever possible, video and audio evidence will be available to the Police and Courts in the event of any of our CEO's/CPA's being subject to incidents of physical or verbal abuse, threats or aggressive behaviour.

The cameras are also being introduced to reduce the number of complaints being made against the officers whereby the allegations made are unfounded.

2. Is there evidence to suggest that the use of BWC reduces incidents of assault or verbal abuse toward CEO's/CPA's?

The decision to introduce these cameras all Woking Borough Council's CEO's/CPA's has been taken as a result of their success in reducing the level of incidents toward CEO's employed in other UK locations.

Studies carried out by Health and Safety Teams also suggest that, in the event of recording being activated by an Officer, there are behavioural changes in those being recorded.

3. How will CEO's/CPA's use these cameras?

The Information Commissioner's Office (ICO) is the regulator of the Data Protection Act 1998 and has issued guidance for the use of BWC.

All CEO's/CPA's will wear body-worn CCTV as part of their uniform. It will be used in an overt manner.

At the commencement of a recording the EEO will give a verbal warning that recording is taking place, although this is not mandatory. As a general rule, where an Officer is in uniform and clearly displaying a camera in operation with the recording light on and the display facing forward to show that recording is active, the ICO would consider that its guidance on the conditions for the use of body-worn equipment has been satisfied.

4. Can less privacy intrusive solutions achieve similar objectives?

The short answer is no. CEO's/CPA's will only use the equipment for one of the following reasons:

• For their own protection when involved in confrontational situations where they believe they may be subject to physical or verbal abuse
• Or when approached in a manner they perceive as aggressive or threatening.

5. What could be done to minimise intrusion for those that may be recorded, particularly if specific concerns have been expressed?

Should a CEO's/CPA's become involved in a situation where recording is considered necessary they will, as far as is reasonable, focus recording on the perpetrator(s) of the incident.

The cameras are mounted on the body around chest height so any recording will be generally in the direction the CEO's/CPA's will be facing which, in most cases, will be face on to the perpetrator(s) but this cannot be fully guaranteed. Any footage taken of a person(s) not involved will be purely coincidental and will not be used for any purpose unless they specifically agree to be a witness. This will be rare and very specific circumstance based.

6. What will Woking Borough Council be doing with recorded images?

Recorded images and audio will be used dealing with officer conduct complaints, reviewing incidents of verbal or physical abuse against our CEO's/CPA's. For incidents where the Police have not been in attendance a decision will be made on whether a referral is appropriate.

All data not deemed as evidence or not required by the Police for possible prosecution will enter a secure short term archive database and will be deleted as per the software settings after 31 days.

Any data retained will only be kept until all investigations have been completed or prosecution has taken place and then deleted after 31 days.

Footage can only be viewed by authorised personnel.

7. How will members of the public be able to view recorded data?

Any request to view captured video by a member of the public, or their legal representatives, should be made in writing to Peter Bryant, Head of Democratic and Legal Services at Woking Borough Council

Requests may also be made through the 'Subject Access Request' procedure.

8. Will body-worn CCTV be used as supporting evidence for the issue of Penalty Charge

Notices?

No. The cameras are being introduced purely as part of the Personal Protective Equipment under Woking Borough Councils Health & Safety policy for CEO's/CPA's.

9. Who ensures that Woking Borough Council follows the correct and proper use of the cameras and footage?

Woking Borough Council has and will continue to work in conjunction with the Surveillance Camera Commissioner's (SCC) office. The SCC is a Government appointed independent Commissioner responsible for all guidance in relation to surveillance camera systems.

They have reviewed and agreed all the policies and operational guidelines issued to staff that will be using the cameras and its software.

As part of this process Woking Borough Council have followed and complied with all legislation and guidance published in the following:

Data Protection Act 1998
Freedom of Information Act 2000
Human Rights Act 1998
Protection of Freedoms Act 2012
Home Office Surveillance Camera Code of Practice Information Commissioners Code of Practice
We will consult the Surveillance Camera Commissioner on any updates or amendments to the policies and operational guidance before they take place.