

Hamilton Police Service Board Use of Body-Worn Cameras Policy P-025

Effective date: October 24, 2024

Reviewed: Amended:

Applicable Legislation

Municipal Freedom of Information and the Protection of Privacy Act, R.S.O. 1990, and Community Safety and Policing Act, 2019, S.O. 2019, c.1, Sched.1 (the Act):

Guiding Principles

The Hamilton Police Service Board (the Board) is committed to providing fair, effective, efficient, equitable and accountable policing to the members of our communities, in accordance with the fundamental rights guaranteed by the *Charter of Rights and Freedoms* and the *Human Rights Code* of Ontario. The Board is also committed to ensuring the inherent worth and dignity of all individuals who come into contact with police is respected in all interactions.

By recording interactions with members of the public and the police, body-worn cameras (BWCs) have been advanced as one way to increase transparency, enhance accountability for rights protections and situations in which force is used and these recordings may also improve law enforcement practices by identifying where a need may exist for additional training, supervision or discipline. BWCs will also enable the timely and fair investigation of any allegations of misconduct by Service Members, and a quick resolution of complaints.

BWCs are effective tools for gathering evidence and providing a more accurate and robust record of events, thus improving the work of the criminal justice system as a whole.

Purpose of Policy

The purpose of this Policy is to direct the Chief to authorize the Service to deploy and use BWCs and to ensure their use by the Service occurs in such a way as to ensure the following public interests are served:

- Improving the transparency of the Service with regards to allegations of discreditable conduct, improper conduct, misconduct, biased service delivery and excessive or improper use of force by Service Members;
- Ensuring the accountability of the Service and Service Members through internal and public oversight systems;
- Protecting individuals' right to privacy by limiting access to recordings from BWCs to the greatest extent possible and to as limited a number of people as possible;
- Ensuring individuals have access to their personal information when it is collected by the BWCs;
- Enhancing public trust and police legitimacy;
- Enhancing public and police officer safety;
- Enhancing the Service's commitment to anti-racist, bias-free service delivery;
- Providing improved evidence for investigative, judicial and oversight purposes;
- Ensuring timely and fair response to misconduct allegations against Service Members, in a manner that enhances public and Member confidence in the Service's complaint process; and
- Providing information as to the effectiveness of Service procedures and training.

Risks and Mitigation

The Board acknowledges the use of BWCs is not without challenges. There are important concerns surrounding privacy, particularly where what could be perceived as surveillance of vulnerable people and racialized communities is concerned, or in sensitive situations such as domestic violence calls.

The Board recognizes that individuals have a justified expectation of privacy as they go about their daily business, even within public spaces, and this expectation must be respected subject to reasonable limits.

In addition, the manner in which BWC use is implemented and governed could have a substantial impact on their effectiveness as it relates to cases of excessive use of force or other matters that may engage the police oversight system. Similarly, access to recordings must also be strictly governed, both to prevent breach of privacy by internal and external individuals, and to ensure all recordings are preserved in their full, unedited form on the system, throughout their retention period. Finally, the transparency of the implementation of this Policy by the Service, including public access to information on its effectiveness in achieving the Policy's goals is a critical element of building the public trust necessary for the achievement of the Policy's purposes and goals.

The Board will monitor the Service's implementation of this Policy to mitigate these risks, including the provision of robust training to Service Members to ensure the effective deployment of this tool. The Board will also continue to monitor best practices and recommendations to identify possible revisions to this Policy and work with the Service, other emergency services, technology partners and the community to identify other opportunities and strategies to achieve the crucial goals of delivering professional policing in a manner that respects the dignity, privacy, worth and human rights of individuals.

Policy of the Board

It is the Policy of the Hamilton Police Service Board that the Chief of Police, in consideration of information provided by the Information and Privacy Commissioner of Ontario and other relevant stakeholders, will develop procedures that:

General

- 1. Implement the recommendations set out in the Office of the Privacy

 Commissioner of Canada's *Guidance for the Use of Body-Worn Cameras by Law*Enforcement Authorities (2015), and ensure new recommendations and best practices continue to be monitored and implemented as they are identified by the relevant provincial and federal authorities.
- Specifically identify the legislative authority for the collection of personal
 information that will be captured by the BWCs and ensure any such collection
 aligns with that authority and all other relevant legislation, including any
 legislative provisions addressing data, information or records storage, access,
 use and/or disclosure.
- 3. Ensure all use of BWCs and their recordings is consistent with the *Ontario*Human Rights Code and the Charter of Rights and Freedoms.

When and How to Use Body-Worn Cameras

- 4. Ensure clear direction in the policies and procedures of who shall be equipped with BWCs and when the cameras shall be activated.
- 5. Provide guidance to officers on when a BWC must be activated, unless an unexpected and immediate threat to the life or safety of the Service Members or a member of the public makes it impossible or dangerous to activate the BWC prior to that interaction.

- 6. Establish within the policies and procedures that BWCs will not be used for general surveillance of members of the public.
- 7. Ensure that clear direction is established within policies and procedures regarding when a Service Member can and cannot deactivate the BWC.
- 8. Ensure that clear guidelines are established within the policies and procedures governing Service Members from intentionally preventing the BWC from capturing video or audio during an interaction with a member of the public, with the sole exception of temporarily covering the lens to protect the dignity of an individual during situations of a sensitive nature.
- 9. Establish that Service Members must inform members of the public that are part of an interaction involving BWCs they are being recorded at the earliest opportunity and that the camera is active and recording.
- Ensure clear guidelines are established within the policies and procedures addressing privacy considerations in situations where there is a heightened reasonable expectation of privacy.
- 11. Establish, with regards to the BWC's 'stealth mode' (i.e., a mode wherein the BWC is recording without providing visible and audible signals) that:
 - a. The 'stealth mode' will only be used in situations where activating the camera in its normal mode may endanger the safety of a Service Member, and only for the duration necessary for this purpose;
 - b. If a BWC was set to 'stealth mode' prior to an interaction with a member of the public to protect the safety of a Service Member(s), and the Service Member subsequently engages with a member of the public, the Service Member must inform that individual or individuals as soon as reasonably possible that the BWC is activated, and turn off the 'stealth mode' as soon as possible.
- 12. Establish that Service Members must upload all recordings from the BWC at the end of their shift, and that supervisors must ensure all recordings from BWCs used by Service Members under their supervision have been uploaded.

Controls

- 13. Establish that if a Service Member has not recorded in full or in part an interaction with a member of the public, the Service Member must document the specific reason a recording was not made in part or in full using a designated process, and that this process must include a review by a Service Member designated by the Chief of Police.
- 14. Establish training requirements for Service Members to fulfill prior to being issued a BWC, and subsequent on-going training requirements, so as to ensure Service Members are able to comply in full with this Policy.
- 15. Establish a comprehensive auditing schedule to govern and ensure compliance with policies and procedures.
- 16. Establish the framework for discipline of Service Members who fail to comply with the policies and procedures governing BWCs.

Transparency

17. Ensure clear and current instructions are posted on the Service's public website providing direction for the public on how to obtain information, details, reports and guidance on the use of BWCs.

Secure Retention and Disposal of Recordings

- 18. In consideration of information provided by the Information and Privacy
 Commissioner of Ontario, and in accordance with all applicable legislation,
 establish and ensure recordings from BWCs, including any meta-data produced
 by the BWCs or the technology supporting the Service's BWCs, will be:
 - a. Stored on a secure Canadian storage server in accordance with all applicable provincial and federal legislation and security best practices, so as to prevent any editing, tampering and unauthorized access to recordings and meta-data;

- Encrypted within the camera during transit to the storage server and while in storage; and
- c. Destroyed at the end of their retention period in a secure manner which prevents recovery and unauthorized access to the recordings and meta-data.
- 19. In consideration of information provided by the Information and Privacy Commissioner of Ontario, and in accordance with all applicable legislation, establish the minimum retention period for recordings from BWCs, and conditions for extensions of the retention period.
- 20. Establish actions to be taken by the Service in the case of a potential or actual access breach of the Service's recording and meta-data storage service, including breach mitigation and control steps, and the steps required to notify the public and impacted individuals of the potential breach.
- 21. Establish that the Information and Privacy Commissioner of Ontario must be notified as soon as reasonably possible of significant privacy breaches, to be determined through consideration of all relevant circumstances, including whether:
 - The personal information at issue is sensitive, either by its nature or given its context;
 - b. The breach is likely to cause significant harm, including financial, reputational, or emotional harm, such as embarrassment or humiliation;
 - c. The breach involves the personal information of a large number of individuals;
 - d. The likelihood the personal information at issue could be misused, or further disseminated by others; or
 - e. The Service is having difficulties containing the breach.

Limited Use and Access to Body-Worn Camera Recordings

- 22. Establish the conditions under which specified individuals may view or receive copies of recordings from BWCs, ensuring that:
 - a. Service Members who wore the BWC which captured a recording may access the recording and make additions to their notes based on the review of the recordings, which must be clearly marked as such, once they have completed any required initial reports, statements and interviews regarding the recorded events;
 - b. Access to recordings by other Service Members is limited only to those with a specified role in relation to the recording which justifies and necessitates such access, including, but not limited to, investigation, supervision, legal proceedings, training development, reporting, and auditing, and will be granted only when circumstances require such access;
 - c. Access to recordings is provided in a timely manner to members of bodies responsible for independent oversight of police (e.g. the Law Enforcement Complaints Agency and the Special Investigations Unit) who are conducting an investigation and who have grounds to believe the recording includes evidentiary materials;
 - d. Access to recordings is provided in a timely manner to individuals who have lawful authority to obtain such access.
- 23. Establish, notwithstanding the provisions of section 22 of this Policy, additional safeguards to enhance the storage and limit the access to recordings of minors who are suspected of an offence or are witnesses to a suspected offence, in accordance with the *Youth Criminal Justice Act*.
- 24. Establish an audit trail will be created and maintained by the Service for records that have been requested.
- 25. Establish that a member of the public may request to view recordings from a BWC or that the recordings and/or their meta-data be released to the requestor.

26. Establish that the Service may only use recordings from BWCs for the purposes of training after the identities of all members of the public captured in the recordings are concealed through measures such as image blurring and voice distortion.

In addition, it is the Policy of the Board that:

- 27. The Chief of Police may initiate release to the public of recordings from BWCs, taking into consideration relevant factors, including what is consistent with the law and public interest, and what is reasonable in the circumstances of the case. The Chief of Police will include, along with the release, a justification of the public interest in releasing the recording. These releases will be in the Chief of Police's purview as per the CSPA versus an MFIPPA release.
- 28. Whenever the Chief of Police initiates the release to the public of any recordings from BWCs that include images or voice recordings of members of the public:
 - a. The identities of all members of the public captured in the recordings are concealed through measures such as image blurring and voice distortion, unless the Service is required by law to release the recordings in another form; and
 - b. The Chief of Police will include, along with the release, a justification of the public interest in releasing the recording.

Furthermore, it is the Policy of the Board that the Chief of Police will ensure:

- 29. Recordings from BWCs will not be used in combination with facial-recognition technology, video analytics software, voice recognition software, or to generate a searchable database of images of individuals who have interacted with Service Members, with the exception of comparing images that are directly related to an investigation to a "mug shot" database in a manner approved by the Board.
- 30. The Service will not use BWC recordings recorded during a protest in combination with the Service's "mug shot" database unless there are reasonable grounds to believe an offence has been committed at the protest, and then, only

- for the purpose of investigating such an offence and comparing only images of the individual suspected of the offence to the images in the database.
- 31. The Service will conduct a Privacy Impact Assessment in consultation with the Information and Privacy Commissioner of Ontario, and bring its findings before the Board for its consideration *prior* to implementing any significant changes to the Service's use of BWCs, including when:
 - a. The Service wishes to utilize recordings from BWCs in a novel manner or in combination with other software or hardware;
 - b. The technology used to capture, retain, store or destroy the recordings changes beyond routine software updates issued by the supplier, including the deployment of any new or additional features; or
 - c. The scope or governance of the Service's BWC program changes.

Auditing

It is also the Policy of the Board that the Chief of Police will:

- 32. Ensure the Service conducts an annual audit:
 - a. That reviews BWC recordings and meta-data for:
 - all incidents for which a complaint under the Community Safety and Policing Act was filed during the reporting period;
 - ii. all incidents for which an investigation was initiated by the Special Investigations Unit or the Law Enforcement Complaints Agency;
 - iii. a sample of incidents for which a Use of Force form was completed during the reporting period;
 - iv. a sample of incidents during the reporting period that were initiated by a call for service;

- v. a sample of incidents during the reporting period that were not initiated by a call for service;
- vi. all incidents wherein a BWC was disabled for the purpose of protecting law enforcement strategies.
- vii. a sample of the meta-data for incidents whose retention period has expired during the reporting period.
- b. Ensure the audit includes a review of BWC recordings for these incidents to ensure that:
 - the recording begins prior to the beginning of the interaction with the member of the public, and if not, that a satisfactory explanation for the failure to activate the BWC before the interaction began was provided in accordance with the Service's Procedure;
 - ii. the subject of the recording is informed at the earliest opportunity in the interaction that the interaction is being recorded for video and audio;
 - iii. any obstruction of the lens or gaps in the recording are justified and of reasonable duration;
 - iv. the recording ends:
 - after conditions for an exception in accordance with section 7 of this Policy have been established; or
 - after the interaction has ended;
 - v. all access to the recordings was justified and necessary;
 - vi. all requests for recordings from the Special Investigations Unit or the Law Enforcement Complaints Agency were fulfilled in full and in a timely manner; and
 - vii. the Service is in compliance with required retention and destruction practices.

33. Advise and file with the Board's' Administrative Director a new copy of the Service's procedure governing BWC use whenever a change is made to the procedure;

Reporting

- 34. Provide the Board with an annual report which will include:
 - a. A summary of any changes to the relevant procedure(s) made in accordance with this Policy over the reporting period;
 - b. The findings of the annual audit;
 - c. The number of complaints received by the Service with regards to the use or failure to use of BWCs, a summary of the complaints, and a summary of the dispositions of the complaints during the reporting period;
 - d. The total number of complaints received by the Service against Service
 Members for which there was a relevant BWC recording, broken down by complaint resolution status;
 - e. The number, if any, of recordings requested by the Special Investigations
 Unit, or the Law Enforcement Complaints Agency, which were not fulfilled
 within 30 days;
 - f. The number of requests made by members of the public to view or release to the public recordings from BWCs which were refused, if any, and a high-level overview of the reasons for any refusals;
 - g. The total number of recordings currently stored by the Service beyond the default retention period, generally categorized by the reason for the extended retention period;
 - h. The total number of recordings released as part of a disclosure process in a legal proceeding;

- i. The number of reports submitted in accordance with section 13 of this Policy, documenting the reason for a failure to activate the BWC prior to the beginning of an interaction with a member of the public, and the number of these incidents, if any, which were found not be in compliance with the procedure;
- j. The number of Service Members disciplined for lack of compliance with BWC policies and/or procedures and a summary of the disciplinary measures used;
- k. The number of investigations into potential privacy breaches during the reporting period and the number of such incidents that were determined to constitute a breach and a summary description of these incidents.
- The costs and/or savings associated with the deployment and use of BWCs in the previous year; and
- m. A review of whether the deployment of BWCs is achieving the purposes set by this Policy, whether their use remains justified in light of these purposes, and whether their use has resulted in any unintended negative impacts, including, but not limited to:
 - i. Use of Force trends over the past five years;
 - ii. complaint trends over the past five years;
 - iii. findings from a survey of public trust in the Service at a timeframe to be determined after a satisfactory implementation period; and
 - iv. findings from a consultation with impacted and marginalized communities.

It is also the Policy of the Board that:

35. The Board will review this Policy within one year after full deployment of the BWCs by the Service, and thereafter, at least once every three years, and make any amendments it determines are appropriate, having regard to the Policy's purposes, insights gained through the Service's deployment and experience with

BWCs, and academic or expert research findings concerning the use of BWCs by the Police Service.	