

Section	Integrated Video and Evidence Program	Current Approval Date
Subject	Body-Worn Camera Standard	Month, Day, Year

## **PURPOSE**

Body-Worn Cameras (BWCs) are forward-facing audio and video recording devices worn by Customer Protection Officers (CPOs), Revenue Protection Officers (RPOs), and Station Safety Ambassadors (SSAs), hereinafter referred to as Authorized Officers, to capture interactions with the public during the execution of their duties. BWCs enhance public trust, improve officer and public safety, and reinforce Metrolinx’s commitment to fair, equitable, and bias-free service delivery. They also support operational workflows by providing accurate, high-quality evidence for investigative, judicial, and oversight purposes.

This Standard, along with the Audio and Video Recording Policy, the Body-Worn Camera Procedure Guide, and the Information Sharing Standard, outlines the principles and requirements for the safe and effective use of BWCs by Authorized Officers during Metrolinx operations.

## **SCOPE AND APPLICATION**

This Standard applies to all Metrolinx Authorized Officers, including full-time, part-time, probationary, and fixed-term employees issued with a Body-Worn Camera (BWC). BWCs must be used to record all safety, investigative, and enforcement activities in accordance with this Standard and the CPS Body-Worn Camera Procedure Guide. BWCs are not used for general surveillance of transit users or individuals on Metrolinx property.

## **BODY-WORN CAMERA EQUIPMENT**

In accordance with guidance from the Information and Privacy Commissioner of Ontario (IPC), Metrolinx follows the technical requirements set out for Body-Worn Cameras (BWCs), supporting that all equipment meets rigorous specifications. This includes high-definition video and audio recording capabilities to capture clear, accurate, and reliable evidence.

To safeguard the integrity of recorded footage, BWCs must use secure data encryption both during transmission and storage, to protect against unauthorized access and/or tampering. Additionally, Metrolinx BWCs shall have clear activation protocols as outlined in the Body-Worn Camera Procedure Guide, with clear visual indicators to show when recording is in progress, thereby supporting transparency and accountability.

Metrolinx aligns with the IPC Model Governance Framework for Police Body-Worn Camera Programs in Ontario. All BWCs are integrated with secure Digital Evidence Management Systems (DEMS), enabling proper handling and storage of recorded footage, including sharing, retention, and disposition of evidence records in alignment with Ontario's privacy laws and Metrolinx’s Records Retention Schedule. These practices are further supported by the Digital Evidence Management System (DEMS) Standard, the Information Sharing Standard, Metrolinx’s Records Retention Schedule, and the Digital Evidence Management System (DEMS) Procedure Guide.

Furthermore, the deployment of BWCs is accompanied by training and comprehensive Standards and Procedure Guides that cover the usage, data access, and public notification requirements. BWC footage shall only be accessed by authorized personnel for authorized purposes; the privacy rights of individuals captured in the footage are respected at all times.

Collectively, these Standards and Procedure Guides reflect a balanced approach that supports the provision of security, safety and effective enforcement of legislation and Metrolinx By-Laws, while safeguarding the privacy and rights of Metrolinx transit users.

## **BODY-WORN CAMERA ACTIVATION AND RECORDING**

BWCs must be activated at the earliest reasonable opportunity during all calls for service and during all transit safety related interactions. This includes but is not limited to crimes in progress,

failure to provide proof of payment while travelling on Metrolinx property or within a fare paid zone, interactions with disorderly or unsafe member(s) of the public and incident investigations (see *Appendix A for BWC Activation Scenario Chart*). BWC activation protocols for Authorized Officers are designed to maintain consistency and accountability, which are further documented in the Body-Worn Camera Procedure Guide.

Authorized Officers must provide verbal notice that recording has started at the beginning of each interaction, except when doing so would jeopardize safety or the integrity of the situation. BWCs feature a yellow visual sticker indicating audio/video recording, along with a visual red light on the front, as well as an audible beep to clearly notify individuals that a recording is in progress. In accordance with IPC guidelines, continuous recording should be maintained throughout the entire interaction, without unnecessary interruptions, to preserve the integrity of the evidentiary record.

Deactivation of the BWC shall only occur once the interaction has fully concluded, and when there is no reasonable expectation of further engagement by the Authorized Officer. Furthermore, any deviations from the required activation of the BWC, as outlined in the Body-Worn Camera Procedure Guide, must be documented in the officer's memo book and will be subject to internal oversight and review. Authorized Officers must not use BWCs to record private conversations between individuals and their legal counsel or capture privileged information such as Canadian Police Information Centre (CPIC) inquiries (see *Appendix C for the BWC Muting Scenarios Chart*). In sensitive situations, such as providing an individual time to get dressed, officers must make all reasonable efforts to obscure the BWC lens (the BWC shall continue to record the audio of the interaction) to preserve the individual's dignity (see *Appendix B for BWC Obscuring Scenarios Chart*).

To maintain transparency and accountability, Metrolinx employs audit trails and metadata tagging as part of its recording practices, as outlined in the Body-Worn Camera Procedure Guide, as well as the Digital Evidence Management System (DEMS) Procedure Guide. Together, these measures further aim to support lawful and transparent enforcement of legislation and Metrolinx By-Laws while protecting individuals' privacy and maintaining public trust.

## DATA MANAGEMENT

Metrolinx manages BWC footage in accordance with a governance framework that balances law enforcement accountability with the protection of individual privacy rights, as set out under the *Freedom of Information and Protection of Privacy Act* (FIPPA). Strict protocols guide the collection, storage, access, and retention of recorded footage, as outlined in the Metrolinx Records Retention Schedule, Digital Evidence Management System (DEMS) Standard, Digital Evidence Management System (DEMS) Procedure Guide, and Information Sharing Standard.

BWC footage may capture personal information such as identifiable visuals (faces, clothing, location, and distinguishing characteristics), and audio (names, conversations, or locations).

All footage must be securely stored using an encrypted Digital Evidence Management System, with strict access controls. Chain-of-custody logs and audit trails are maintained to support transparency and protect the integrity of the footage.

Authorized Officers are required to activate their BWCs, as per scenarios listed in the *BWC Activation Scenario Chart in Appendix A*, during all specified interactions. In addition, CPOs must activate their devices during all arrests and/or use-of-force incidents. Retention periods for recorded footage vary depending on their nature, with non-evidentiary footage typically deleted after a fixed period as per the Metrolinx Records Retention Schedule, while footage used for the purposes of supporting criminal investigations, safety incidents or formal complaints may be retained for longer.

## PRIVACY CONSIDERATIONS

Protecting individual privacy is a critical component of Metrolinx's BWC Program, as these devices capture real-time, sensitive interactions between Authorized Officers and members of the public. Particular attention is given to scenarios involving vulnerable individuals, such as minors, victims of crime, those experiencing mental health crises, and/or individuals in medical emergencies. To mitigate privacy risks, Metrolinx requires all Authorized Officers to provide verbal notification of the recording at the beginning of the interaction, unless doing so would compromise safety or the integrity of an investigation.

As mandated under FIPPA, any footage containing personal information must be collected lawfully, used only for authorized purposes, and protected from unauthorized access or disclosure. Metrolinx shall not employ the use of BWCs in private areas such as a washroom, except in exigent circumstances.

When BWC footage is shared through Freedom of Information (FOI) requests, redaction techniques, such as blurring faces or muting audio, are applied to safeguard third-party identities.

Data minimization principles are also emphasized, maintaining that only relevant footage is retained, and that non-evidentiary content is removed in accordance with established retention periods identified in the Metrolinx Records Retention Schedule.

Furthermore, oversight by the IPC, Metrolinx's Internal Audit function, Metrolinx's Privacy

Office, and CPS Risk and Audit in conjunction with other Metrolinx business units help maintain that BWC use remains transparent, proportionate, and compliant with legal and ethical standards, balancing the need for officer accountability with the public's privacy rights.

## **REVIEW AND USE OF FOOTAGE**

The review and use of BWC footage are governed by strict protocols aimed at supporting transparency, accountability, and integrity. BWC footage will be used primarily for evidentiary purposes, including but not limited to criminal or safety-related investigations, court proceedings, and/or internal reviews concerning the conduct of Authorized Officers. On occasion and following consultation with the Privacy Office, BWC footage may also be used for safety campaigns, and/or training purposes provided that it remains compliant with applicable privacy laws and respects the privacy of those involved to the extent reasonably possible.

The use of recordings for secondary purposes is generally not permitted under FIPPA and other applicable legislation and regulations, and should be strictly limited. The use of BWC footage for personal use, or to cause harm or embarrassment to individuals, is strictly prohibited.

## **LAW ENFORCEMENT REQUESTS FOR FOOTAGE**

BWC footage may be shared with law enforcement agencies in the support of investigations. Any sharing of footage will be done in accordance with FIPPA, the Information Sharing Standard, and the Information Sharing Procedure Guide.

Authorized personnel, such as the CPS Vice President, CPS Directors, CPS Managers or CPS Investigators, may review footage to corroborate officer reports, evaluate arrest and/or use-of-force incidents, or investigate public complaints and misconduct allegations. All access to footage is logged in the Digital Evidence Management System (DEMS), creating an auditable trail that deters misuse and supports transparency.

## **INTERNAL USE OF FOOTAGE**

BWC footage may also be reviewed for training purposes or as part of performance evaluations for Authorized Officers, provided such use aligns and complies with applicable employee labour relation practices and the Metrolinx Enterprise Privacy Policy. Where the use of BWC footage is approved for training purposes, anonymizing measures will be taken to protect the identity and dignity of those captured in the footage, such as face blurring in compliance with FIPPA and applicable privacy regulations.

## **PUBLIC REQUESTS FOR FOOTAGE**

In accordance with FIPPA, the right of public access to footage from a BWC is a critical component in promoting transparency, accountability, and public trust in Metrolinx enforcement actions. Any release of footage is subject to a thorough review process to maintain the privacy of individuals captured in the footage is protected through appropriate redactions. Public access to footage may be initiated through formal requests, as per FIPPA, and processed

through the Metrolinx Freedom of Information (FOI) Office.

While the release of BWC footage can help clarify the nature of interactions between Authorized Officers and the public, it can also potentially raise legal, ethical, and operational challenges. These include balancing transparency with privacy rights, managing public expectations, and maintaining the integrity of judicial proceedings.

To address these concerns, all BWC footage shall be vigorously vetted, redacted, and in certain instances, will require senior management level approval, before being released to the general public. The release of any BWC footage shall be processed in accordance with FIPPA requirements.

Requests for BWC footage from the public or media are managed through the Metrolinx Freedom of Information Office (FOI). Any disclosure is subject to redaction requirements to protect personal privacy, oversight bodies, such as the IPC, provide guidance on how Metrolinx shall monitor BWC footage, as well as how footage is reviewed and used, supporting that practices align with FIPPA and other applicable legislation and regulation, as well as public expectations of accountability.

Public requests for access to BWC footage will be handled by the Metrolinx FOI Office, in accordance with FIPPA requirements and best practices.

## **TRAINING REQUIREMENTS**

The successful implementation of the Body-Worn Camera (BWC) Program requires comprehensive training to support all Authorized Officers, as well as relevant Managers, Investigators, and administrative staff, understand the operational, legal, and ethical responsibilities of BWC use.

In-person training is mandatory for all personnel required to wear or manage BWC equipment and footage. This includes detailed instructions on the technical operation of the devices, covering activation, deactivation, camera positioning, troubleshooting, and secure footage upload to the Digital Evidence Management System (DEMS). Training will be conducted in a testing environment to minimize potential privacy intrusions when capturing test footage on the BWCs.

Authorized Officers shall also receive in-depth guidance on the legal framework governing BWC use, including privacy rights under FIPPA and the *Canadian Charter of Rights and Freedoms*, as well as the rules of evidence and disclosure relevant to legal proceedings. Scenario-based training will support Authorized Officers in making sound decisions in complex real-life situations, such as determining when to record, managing interactions with vulnerable individuals, and responding to public questions about recording. Managers and Investigators will receive training in footage review procedures, access controls, redaction techniques, and chain of custody protocols.

Refresher training shall be delivered regularly to reinforce policy, standards, procedures and adapt to changes in legislation, technology, or operational requirements. All training will

emphasize the ethical responsibilities of using BWCs, focusing on transparency, professionalism, and maintaining public trust.

## **COMPLIANCE AND ACCOUNTABILITY**

Compliance and accountability are essential to the successful implementation of Metrolinx's BWC Program, maintaining that the technology is used both lawfully and ethically. Metrolinx has established a comprehensive compliance framework that includes clear standards, policies, and procedures that define when and how cameras are to be used, the secure handling of footage, and the consequences of misuse or non-compliance. Routine audits will be conducted as per the Audit Program Standard to monitor compliance.

Authorized Officers shall be held accountable for activating their BWCs during all required interactions as outlined in the Activation Scenario Chart in Appendix A. Any failure to activate the BWC as required must be documented with a justifiable explanation.

The associated Digital Evidence Management System features role-based access controls and audit trails that logs all activity related to the viewing, editing, or sharing of footage. This provides a transparent record for oversight.

Compliance also includes meeting Metrolinx record retention and privacy obligations and the appropriate handling of personal information. This involves secure storage, timely disposal of footage, and the redaction of personal information in response to FOI requests.

Independent oversight agencies, such as the IPC, may audit or investigate the Metrolinx BWC Program to maintain it meets legal standards and respects ongoing reporting through an annual public report, accountability metrics, and public communication further strengthen the integrity of the Metrolinx BWC Program, reinforcing public trust and enhancing public safety.

## **TECHNICAL SUPPORT AND MAINTENANCE**

The successful implementation and sustainability of Metrolinx's BWC Program requires robust technical support and comprehensive maintenance infrastructure. This includes the acquisition and upkeep of camera hardware, secure data storage systems, software footage management, and reliable chain of custody processes to maintain evidentiary integrity.

BWCs must be regularly inspected, cleaned, and updated with firmware patches provided by manufacturers to address bugs and security vulnerabilities on a regular basis. Data retention best practices outlined by the IPC require that all recorded footage be securely stored in encrypted cloud-based environments that comply with Canadian privacy standards.

Metrolinx IT personnel and technical support staff are essential for implementing cybersecurity controls, storage capacities, and assisting in managing device malfunctions.

Authorized Officers shall also receive ongoing training to support correct camera operation, manage footage, and troubleshoot common issues.

Additionally, Metrolinx Cybersecurity shall perform periodic vendor compliance reviews and threat risk assessments to confirm that BWC systems comply with Metrolinx cybersecurity policies and control requirements, thereby mitigating the risk of data breaches.

## **ROLES AND RESPONSIBILITIES**

### **CPS Vice President**

The CPS Vice President is responsible for the following:

- Providing oversight and overseeing the consistent application of this Standard.

### **CPS Director, Professional Standards**

The CPS Director, Professional Standards is responsible for the following:

- Overseeing compliance with this standard and all associated procedures.
- Communicating and implementing the Standard and associated Procedure Guide to applicable Metrolinx employees.
- Report issues of non-compliance to the relevant Metrolinx business unit.

### **Authorized Officers**

Authorized Officers (Customer Protection Officers (CPOs) Revenue Protection Officers (RPOs) & Station Safety Ambassadors (SSAs) are responsible for the following:

- **Equipment Readiness:** Assigned equipment is operational and maintained in accordance with the CPS - Issued Work Equipment SOP.
- **Proper Usage:** Operate equipment in accordance with established protocols, including activation, obscuring, muting, and deactivation procedures.
- **Digital Evidence Management:** Upload footage in a timely and accurate manner in accordance with CPS data management procedures including metadata tagging.
- **Evidence Integrity:** Maintain the integrity of footage by following proper handling procedures and maintaining that footage is not altered, deleted, or mishandled.
- **Documentation:** Making memo book notes to support any deviation from the BWC Standard or Body-Worn Camera Procedure Guide.

### **CPS Managers**

CPS Managers are responsible for the following:

- Providing coaching to Authorized Officers.
- Conducting routine audits of Authorized Officer BWC recording footage.
- Review all footage related to all arrests and/or use of force events.
- Monitoring Authorized Officer compliance with BWC activation, usage, and upload procedures as stated in the Body-Worn Camera Procedure Guide.
- Escalate issues of non-compliance to the CPS Director, Professional Standards.

## **CPS Logistics**

CPS Logistics are responsible for the following:

- Coordinating the physical maintenance and maintaining storage of in-field and spare BWCs.

## **CPS Data & Analytics Team**

The CPS Data & Analytics Team is responsible for the following:

- Reporting program performance and statistics (generating reports).
- Approving permissions for BWC software based upon a role-based access control matrix as stated in the Digital Evidence Management System (DEMS) Standard and supporting procedure.

## **CPS Training and Development**

The CPS Training & Development Team is responsible for the following:

- The development and implementation of a robust training program which supports Authorized Officers are properly equipped to operate BWCs, including refresher training.
- Periodically reviewing and updating training material as required.

## **CPS Risk and Audit team**

CPS Risk & Audit is responsible for the following:

- Conduct routine and follow-up audits as per the Audit Program Standard to support that the BWC Program adheres to Metrolinx Policies, privacy regulations, Standards, and IPC guidelines.
- Developing recommendations to address noncompliance.
- Supporting the development of Corrective Action Plans (CAPS) that will support that issues of noncompliance are addressed fully and in a timely manner.

## **ESCALATIONS AND EXCEPTIONS**

Any exceptions or instances of non-compliance with this Standard shall be escalated to the Director of Professional Standards. Failure to comply with this Standard or the affiliated procedures may result in disciplinary action, up to and including dismissal.

## REFERENCES

Audit Program Standard

Body-Worn Camera Procedure Guide (CSM-0202-02(P))

*Canadian Charter of Rights and Freedoms*

Digital Evidence Management System (DEMS) Standard (CSM-0202-06)

Digital Evidence Management System (DEMS) Procedure Guide (CSM-0202-06(P))

*Freedom of Information and Protection of Privacy Act (FIPPA)*

Information Sharing Procedure Guide (CSM-0202-08(P))

Information Sharing Standard (CSM-0202-08)

IPC Model Governance Framework for Police Body-Worn Camera Programs in Ontario

Audio and Video Recording Policy (CSM-0202-01)

Metrolinx Information Security Policy (CA-0504-02)

Metrolinx Enterprise Privacy Policy (CA-0901-01)

Metrolinx Records Retention Schedule

## ADMINISTRATION

Identification Name	Body-Worn Camera Standard
Approved By	Chief Operating Officer
Owner	Vice President, Customer Protective Services
Monitor	Director, Professional Standards, Customer Protective Services
Original Approval Date	
Review Frequency	Annually
Supersedes	N/A

## STANDARD HISTORY

Revision / Review Date	Author	Description
December 10, 2025	Customer Protective Services, Professional Standards	New Standard

## DEFINITIONS

**Accidental:** An event which occurs inadvertently, or unexpectedly.

**Activate:** A process which causes the Body-Worn Camera to capture audio and/or video footage.

**Authorized Officer:** Is an individual who has been formally granted the authority to act on behalf of Metrolinx as a Customer Protection Officer (CPO), Revenue Protection Officer (RPO) or a Station Safety Ambassador (SSA).

**Body Worn Camera (BWC):** A device worn by an Authorized Officer for the purpose of recording video and audio information.

**Call for Service:** A dispatch log entry which has been assigned to a specified Authorized Officer for a field response.

**Corrective Action Plans (CAPs):** Detailed, structured approach that outlines the steps an organization will take to address and resolve issues identified during an audit or other evaluation process.

**Customer Protection Officer (CPO):** A person employed by Metrolinx who has been appointed by the Commissioner of the Ontario Provincial Police (OPP), and approved by the Solicitor General, as a "Special Constable" in accordance with S. 92 of the *Community Safety and Policing Act*, with powers and duties as set out in the appointment.

**Deactivate:** A process which causes the Body-Worn Camera to stop capturing audio and/or video footage.

**Evidence Record:** A comprehensive collection of evidence, which includes documents, physical objects, and electronic data used to establish or disprove a fact in a legal or formal context.

**Footage:** The audio and video recording created by a Body-Worn Camera affixed to an officer's uniform, capturing their perspective of an event.

**Exigent Circumstances:** Refers to urgent, emergency situations that require immediate action to protect public safety, prevent harm, or preserve evidence.

**Manager:** An employee who is responsible for directing, supervising, and monitoring the work of Customer Protection Officers, Revenue Protection Officers, and/or Station Safety Ambassadors.

**Mute:** To stop or disable the audio recording function while the video recording continues.

**Obscure:** The act of blocking, hindering, or preventing the device from capturing a clear video recording.

**Privileged Information:** Refers to information that is protected from disclosure, even if it might be relevant to a case, due to specific legal rules or principles.

**Redaction:** A process to obscure or remove parts of a record, such as personal information, prior to publication or release.

**Revenue Protection Officer (RPO):** A person employed by Metrolinx who carries out Metrolinx Fare Non-Compliance Interactions in accordance with the proper escalation procedure and engages with passengers and assists with fare-related or general questions.

**Secondary Use:** Any use of information beyond the purposes identified at the point of collection in a notice of collection, public privacy notice, or informed consent process.

**Station Safety Ambassador (SSA):** Uniformed Metrolinx employees responsible for detecting and deterring disorder and protecting the safety and security of customers and employees throughout Metrolinx properties.

**Vulnerable Person(s):** A person who is believed to be someone in need of special care due to: cognitive, physical, intellectual, or developmental disability; needing protection from themselves or others; or any other condition/state which may place them at increased risk (e.g. a person perceived to be under-housed/experiencing homelessness, experiencing poverty, experiencing substance use issues, etc.).

## **APPENDIX**

Appendix A: Body-Worn Camera Activation Scenario Chart

Appendix B: Body-Worn Camera Obscuring Scenario Chart

Appendix C: Body-Worn Camera Muting Scenario Chart

**Appendix A: Body-Worn Camera Activation Scenario Chart**

<b><u>CPO</u></b>	<b><u>RPO</u></b>	<b><u>SSA</u></b>
Failure to provide valid proof of payment while in a fare paid zone (A failed fare inspection)	Failure to provide valid proof of payment while in a fare paid zone (A failed fare inspection)	Failure to provide valid proof of payment while in a fare paid zone (A failed fare inspection on a station platform)
Disorderly or unsafe behaviour by a member of the public	Disorderly or unsafe behaviour by a member of the public	Disorderly or unsafe behaviour by a member of the public
Safety related incidents	Safety related incidents	Safety related incidents
Evidence collection and investigation	An incident where if safe to do so, the Authorized Officer believes that a recording may help to document an incident or enhance transparency	An incident where if safe to do so, the Authorized Officer believes that a recording may help to document an incident or enhance transparency
Crimes in progress		
Fatality Response and Scene Management		
Mental Health Apprehension		
All other interactions where the interaction is for a safety, investigative, or enforcement purpose		

**Appendix B: Body-Worn Camera Obscuring Scenario Chart**

<b><u>CPO</u></b>	<b><u>RPO</u></b>	<b><u>SSA</u></b>
To preserve the dignity of an individual in sensitive situations (interacting with an individual who is having a Mental Health Crisis to preserve their dignity)	To preserve the dignity of an individual in sensitive situations	To preserve the dignity of an individual in sensitive situations
Attending to a seriously injured person receiving care	Attending to a seriously injured person receiving care	Attending to a seriously injured person receiving care
CPIC Checks		

**Any obscuring event involving a BWC must be verbally noted in the BWCs audio recording and documented in the Authorized Officer’s memo book immediately once it is safe to do so.**

**Appendix C: Body-Worn Camera Muting Scenario Chart**

<u>CPO</u>	<u>RPO</u>	<u>SSA</u>
Private, medical, investigative, or confidential employment-related discussions	Private, medical, investigative, or confidential employment-related discussions	Private, medical, or confidential employment-related discussions
CPIC Checks		
Conversations between an arrested/apprehended individual and their legal counsel		

**Any muting event involving a BWC must be documented in the Authorized Officer's memo book immediately once it is safe to do so.**