APPENDIX C: TECHNOLOGY-SPECIFIC SURVEILLANCE USE POLICY FORM (ONLY TO BE USED FOR NEW TECHNOLOGIES NOT ADDRESSED IN THE SURVEILLANCE USE POLICY)

Division or Unit (if applicable):	Somerville Police Department
Compliance Officer:	Jeffrey DiGregorio, Administrative Captain
Submitted by:	Shumeane Benford, Chief
Date:	June 4, 2026
Surveillance Technology:	Body Worn Cameras

A. **Purpose:** the specific purpose(s) for the surveillance technology:

Identifying, apprehending, and prosecuting criminal offenders;

i. Gathering evidence of violations of any law in criminal, civil, and administrative proceedings;
ii. Providing information to emergency personnel; and
iii. Documenting and improving performance of City employees.

1. **Authorized use:** the uses that are authorized, the rules and processes required before that use, and the uses that are prohibited:

Officers wearing body worn cameras are to record all law enforcement interactions with civilians. Whenever possible, officers should inform individuals that they are being audio and video recorded at the beginning of the encounter. In locations where individuals have a reasonable expectation of privacy, such as a residence, individuals may request not to be recorded. In such cases, the officer(s) shall have discretion not to record the event based on the purpose and circumstances of their presence or to utilize BWCs in a less intrusive manner, such as deploying audio-only recording or averting the camera away from minors, victims, or others in a vulnerable condition. Otherwise, the body worn camera shall remain activated until the event is completed in order to ensure the integrity of the recording. If an officer does not record an event, they must provide a written explanation as to why they did not.

BWCs may not be used to surreptitiously record people or conversations or to record (1) communications with other police personnel, (2) non-law enforcement activities or officers' personal activities, (3) confidential information, (4) within the police station absent exigent circumstances, or (5) First Amendment protected activities absent specific indicia of unlawful activity.

2. **Data collection:** the surveillance data that can be collected by the surveillance technology:

Body worn cameras are intended to record all contacts police officers have with citizens in the performance of their official duties. The devices will capture audio and video recordings of police contacts, conversations, and other engagements with civilians. The BWCs are to be worn, activated, and the resulting data processed and accessed in accordance with police department policy. The cameras shall be worn in an open and apparent location and not used as surreptitious recording devices. The body worn camera shall be activated prior to initiating contact with the citizen, and at the initiation of any other law enforcement or investigative encounters. Officers may use their discretion when deciding to activate the BWC in private or sensitive locations. Officers are not to activate their BWC when conducting ordinary

activities or other situations that do not involve the delivery of police services. Officers may only activate the cameras at public demonstrations when they have an articulable basis to believe unlawful activity may occur. Officers shall only use body worn cameras within the context of existing and applicable federal, state, and local laws, regulations, and Somerville Police Department Rules and Regulations and Policies and Procedures.

3. **Data protection:** the safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms:

   Use of this technology falls under the guidelines established in the City's Surveillance Technology Use Ordinance and the Somerville Police Department's BWC Policy on usage. The Department's BWC Policy requires BWC data be securely downloaded at the end of each shift and establishes a data management structure overseen by a superior officer. The designated superior officer and civilian support staff will be utilized to administer day-to-day access to camera footage in consultation with the Law Department, where appropriate. BWC data shall be maintained on a secure, local or cloud-based server that is password protected, and accessible only to the Chief and the designated superior officer. Officer access to footage may only be granted with the approval of the Chief or designee. Public access will be granted through the Law Department's Public Records Request process. No Surveillance Data shall be stored, accessed, or transmitted without proper encryption, access and password controls.

4. **Data retention:** the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason that retention is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period has elapsed, and the conditions that must be met to retain information beyond that period:

   All files shall be securely downloaded periodically no later than the end of each shift or work period. Each file shall contain information related to the date, body worn camera identifier, and assigned officer. Files should be securely stored in accordance with state records retention laws and retained no longer than useful for purposes of training or for use in an investigation or prosecution. The recordings will be preserved based on the content of the recording (e.g. street encounter, arrest, criminal investigation) and a retention schedule contained in the Department's BWC Policy, which was developed based on the state's records retention schedule.

   The Department shall retain all body worn camera footage or recordings based on the below retention schedule:

   A. Schedule I - Indefinite Retention
      - A.1. Death Investigation
      - A.2. Use of Deadly Force
      - A.3. Motor Vehicle Accident - Fatal
      - A.4. Sexual Assault/Abused Person
   B. Schedule II - 7 Year Retention
      - B.1. Use of Force
      - B.2. Arrest
      - B.3. Felony – No Arrest
      - B.4. Motor Vehicle Accident – Hit and Run/Personal Injury
      - B.5. Incidents that result in employee disciplinary matters
   C. Schedule III - 3 Year Retention
      - C.1. Misdemeanor – No Arrest
      - C.2. Motor Vehicle Accident – Property Damage

C.3. Investigate Person
C.4. Investigate Premise
C.5. Significant Event – Public Safety

D. Schedule IV – 1 Year Retention
D.1. Traffic Stop
D.2. Encounter/Field Interview Observation (FIO)
D.3. Sick Assist

E. Schedule V – 6 months
E.1. No Report - Dispatch / On Site

F. Schedule VI – 30 Day Retention
F.1. Test/Training

Recordings relevant to the following proceedings are to be retained until final disposition of any of the following actions:

A. Arbitration
B. Administrative Agency investigations or litigation
C. Civil suits
D. Criminal investigations, charges or court actions

5. **Public access:** if and how collected surveillance data can be accessed by members of the public, including criminal defendants:

The City shall comply with its obligations pursuant to the Massachusetts Public Records Law, (G. L. c. 4, § 7 cl. 26, and G. L. c. 66, § 10 et seq.) and any other applicable law, regulation, or order of a court or state or federal administrative agency of competent jurisdiction that requires the disclosure of particular Surveillance Data.

Members of the public can make a Public Records Request in writing through the Department's Records Clerk or the City's Records Access Officer. This request is then forwarded to and/or reviewed by the City of Somerville Law Department, who will issue a response subject to applicable exemptions, if any, under the Public Records Law. If the video becomes evidence in a criminal prosecution, the defendant would have additional access rights pursuant to court rules and applicable law.

6. **Third-party data-sharing:** if and how other city or non-city entities can access or use the surveillance data, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the surveillance data:

Video evidence could be shared depending on the investigation and if other law enforcement agencies are involved or affected or if there is a public safety threat. When submitting images/video as evidence for a criminal case, the data would be shared with the District Attorney's Office and disclosed to defendants as required by law. Images could be shared if there was a joint investigation with another Law Enforcement agency, the State Police or the FBI. Images would only be shared with authorized members of the investigating group who had permission to view the video evidence. Recordings will also be made available to police oversight bodies acting within the scope of their jurisdiction.

All access to body worn camera data (images, sounds, and metadata) must be specifically authorized by the Somerville Chief of Police or their designee, and all access is to be audited to ensure that only authorized users are accessing the data for legitimate and authorized purposes. As noted immediately

above, the recordings may also be made available to the public under the Commonwealth's Public Records Law.

7. **Training:** the training, if any, required for any individuals authorized to use the surveillance technology or to access information collected by the surveillance technology, including whether there are training materials:

   Officers assigned to wear Body Worn Cameras will complete a Police Department approved or provided training program before utilizing a camera in the field. Periodic training will continue to occur to ensure effective use and operation of BWCs and that the cameras are being used consistent with the PD's BWC Policy. As established in the City's Surveillance Technology Use Policy, "The Chief of Police, or their designee, shall ensure that all department personnel successfully complete training which the Chief of Police deems necessary to successfully operate and monitor Video Surveillance Equipment".

8. **Oversight:** the mechanisms to ensure that the surveillance use policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the surveillance technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy:

   This technology is under the direction and authorization of the Chief of the Somerville Police Department. The Surveillance Technology Use Policy, all SPD policies and all applicable Massachusetts laws apply. Under the Department's BWC Policy, one superior officer will be assigned to monitor and oversee access to the BWC recordings. This superior officer will have access to and control of the recordings and will keep an access log of all individuals that request or obtain access to recordings. Use of BWCs and compliance with the Department's BWC Policy will be monitored through random audits conducted by the designated superior officer. Failure to adhere to policy and misuse of this technology would result in discipline up to and including termination depending on the nature, severity, and frequency of such violations.