DRAFT – City of Somerville Surveillance Use Policy
Version 1.1 as of 1/16/2019

This Surveillance Use Policy (the "Policy") is issued on _____ (the "Effective Date") by the Mayor of the City of Somerville (the "City") pursuant to Chapter 10 Article III, Section 10.64 of the Somerville Code of Ordinances (the "Ordinance"). The Ordinance provides for the regulation of the City's use or acquisition of Surveillance Technology for the collection, use, and retention of Surveillance Data as defined in Section 10.62 of the Ordinance. Any City Department Head, as defined below, whose department uses or anticipates acquiring or using Surveillance Technology or Surveillance Data, is required to comply with the Ordinance and this Policy. The goal of this Policy is to balance the capacity of Surveillance Technology to improve the delivery of City services with the importance of maintaining individual(s)' right to privacy.

I. Definitions

All capitalized terms in this Policy shall have the meaning given to them in the Ordinance with the exception of the below-defined terms.

A. **Department Head** shall mean the Department Head of any City department which uses or anticipates acquiring or using Surveillance Technology or Surveillance Data.
B. **Compliance Officer** shall mean a person assigned by a Department Head to keep and maintain records on the acquisition and use of Surveillance Technology or Surveillance Data by that City department, including records on access to Surveillance Data, to ensure that the requirements of the Ordinance and this Policy are followed.

II. Oversight

The Department Head of each City department which currently possesses, uses or anticipates seeking to acquire or use Surveillance Technology shall submit to the Mayor the name of a designated Compliance Officer assigned by the Department Head to keep and maintain records on the acquisition and use of Surveillance Technology or Surveillance Data by that City department, including records on access to Surveillance Data to ensure that the requirements of the Ordinance and this Policy are followed.

The Department Head or Compliance Officer for that City department shall be responsible for internal record keeping on the acquisition and use of Surveillance Technology or Surveillance Data by that City department, including records on access to Surveillance Data, to ensure compliance with this Policy.

1. Permissible Purposes and Authorized Uses for Surveillance Technology in All City Departments

A. It is the City's policy that Surveillance Technology or Surveillance Data may be used for, but is not limited to, the following purposes:

i. Identifying and preventing threats to persons and property and preventing injury to persons or significant damage to property;
ii. Identifying, apprehending, and prosecuting criminal offenders;
iii. Gathering evidence of violations of any law in criminal, civil, and administrative proceedings;
iv. Providing information to emergency personnel;
v. Documenting and improving performance of City employees;
vi. Executing financial transactions between the City and any individual engaged in a financial transaction with the City;
vii. Preventing waste, fraud, and abuse of City resources;

viii. Maintaining the safety and security of City employees, students, customers, and City-owned or controlled buildings and property;
ix. Enforcing obligations to the City;
x. Operating vehicles for City business;
xi. Analyzing and managing service delivery;
xii. Communicating among City employees, with citizens, or with third parties; and
xiii. Surveying and gathering feedback from constituents.

B. City Departments may not acquire, use, or enter into an agreement to acquire, share or otherwise use, Surveillance Technology or Surveillance Data without prior approval from the City Council, pursuant to Ordinance Section 10.65(a), unless exempted or excepted from the requirements pursuant to Section 10.63.

C. Use of any Surveillance Technology for any purpose not permitted by the Ordinance is prohibited

2. Process for Approval and Authorizing Use of Surveillance Technology and Surveillance Data

A. The departments that use, or propose to acquire or use, Surveillance Technology or Surveillance Data, must submit to the Mayor's office a report that details the following: the purposes for which the particular Surveillance Technology is used, the nature of the Surveillance Data the Surveillance Technology collects, and information as to whether the minimum amount of Surveillance Data necessary is being collected. If any employee, agent, or contractor of any City department becomes aware of any inaccuracies concerning the use of Surveillance Technology or Surveillance Data that is collected by a department's Surveillance Technology other than as outlined in that City department's report to the Mayor, that employee, agent, or contractor is required to immediately report the collection of such Surveillance Data or use of such Surveillance Technology to the department's Compliance Officer, the Department Head, the Mayor, the City Solicitor, or the Personnel Director.

B. In addition to the internal report detailed above in section III.2.A., Departments Heads shall be responsible for submitting to the Mayor the following documents required by the Ordinance:

i. **Surveillance Technology Impact Report(s)** (Ordinance Section 10.65), in the form provided in Appendix A attached hereto, submitted for each proposed acquisition or use of Surveillance Technology.
ii. **Annual Surveillance Report(s)** (Ordinance Section 10.66), in the form provided in Appendix B attached hereto, submitted annually by the Mayor to the City Council covering the prior calendar year. The first such report, describing all existing Surveillance Technologies and Surveillance Data is due to the City Council 12 months after the effective date of the ordinance. Thereafter, the report will be due to the City Council by May 31 of each year. The annual report shall include a disclosure of any agreements made in the previous year with any non-city entities that may include acquiring, sharing, or otherwise using surveillance technology or the surveillance data it provides (Ordinance Section 10.66(b)(9)).
iii. **Technology-Specific Surveillance Use Policy(ies)** (Ordinance Section 10.65), in the form provided in Appendix C attached hereto, submitted for each proposed acquisition or use of Surveillance Technology not already covered under this Policy. All Technology-Specific Surveillance Use Policies shall be consistent with the provisions set forth in this Policy as it may be amended from time to time. To the extent there is a conflict between this Policy and a Technology-Specific Surveillance Use Policy, this Policy shall govern.

When providing any of the above reports, a Department Head should pay particular attention to

the impacts the use of the Surveillance Technology has on marginalized communities in the City, including, but, not limited to, communities of color. For any disparity that exists, the Department Head shall explain its understanding as to why the disparity exists and how the Department Head intends to address the disparity.

3. Data Collection.

Surveillance Technology produces Surveillance Data upon which the City relies for governmental functions. It is the policy of the City to ensure that the Surveillance Technology it uses collects no more Surveillance Data than is necessary to achieve the specific, authorized purposes of that particular Surveillance Technology.

4. Data Access.

City employees may only have access to Surveillance Data when such access is necessary for their official duties. The Department Head or Compliance Officer of each City department shall report to the Information Technology Department ("ITD"), the Mayor and the City Solicitor, the name of each employee, contractor, or other agent that requires access to Surveillance Data. The Department Head or Compliance Officer shall state the specific Surveillance Data to which each individual may have access. The City may, at any time, with or without notice to the individual, terminate any individual's access to Surveillance Technology or Surveillance Data.

5. Data Protection.

No Surveillance Data shall be stored, accessed, or transmitted without proper encryption, access and password controls, and access-oversight approved by the City's Chief Information Officer or his/her designee in ITD. Each City department's Compliance Officer shall complete and submit to ITD a list of each type of Surveillance Technology currently used by that department, the Surveillance data it collects, the staff who have access to the Surveillance Data, and all other information required under Subsection A above. ITD shall ensure that proper procedures are in place to protect all Surveillance Data. In the event that any department is, in the judgment of ITD, unable to implement the security measures necessary to adequately protect Surveillance Data, ITD shall immediately contact the Mayor and the City Solicitor, and propose additional measures to protect Surveillance Data from inadvertent or unauthorized disclosure.

6. Data Retention.

Surveillance Data will not be maintained any longer than is necessary to achieve its approved purpose(s), provided that the City will retain Surveillance Data for the periods required by the Massachusetts Public Records Law, G.L. c. 66, § 10, the Massachusetts Municipal Records Retention Schedule, or any other applicable laws or regulations.

Exceptions to the Massachusetts Municipal Records Retention Schedule may be requested from the Commonwealth by the City Solicitor at the request of a Department Head as follows:

A. A Department Head may seek exceptions for a particular type of Surveillance Data by seeking the exception explicitly in a Surveillance Technology Impact Report or Technology-Specific Surveillance Use Policy; or
B. A Department Head may seek an exception for a particular type of Surveillance Data from the Mayor on a case-by-case basis.
C. All exceptions and the reasons therefor shall be included in a department's Annual Surveillance Report.

7. Public and Third-Party Access.

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.

The City's intent is to make as much information as possible available to the public without compromising the privacy of any Identifiable Individual(s), as defined in Section 10.62 of the Ordinance. The City shall, to the extent possible and permitted in accordance with applicable laws and regulations, anonymize, aggregate, and/or geomask Surveillance Data where necessary to protect the privacy of Identifiable Individuals. While some data may not on its own reveal the personal information of Identifiable Individuals, when combined with other data it may reveal information that would otherwise be exempt from disclosure by law. In the event that a City employee suspects that the release of data would present such a risk, the employee shall report that risk to the Department Head or the Compliance Officer for that employee's department and the Department Head or the Compliance Officer shall contact the Mayor and City Solicitor requesting a legal opinion from the City Solicitor as to whether the data is exempt from disclosure under the Public Records Law or other applicable law or regulation.

Surveillance Data may only be accessed by authorized City employees, as described in Section III.4. above, and may only be distributed to third parties in accordance with this Section 7 of this Policy. However, any department may share Surveillance Data with the Police Department under Exigent Circumstances.

8. Training.

Upon beginning employment or within a reasonable time after commencing employment, any City employees or City contractor who will be involved in the collection of Surveillance Data or use of Surveillance Technology will be given a copy of the Surveillance Ordinance and this Policy for their review and trained by their Department Head, supervisor, or other appropriate person assigned to conduct such trainings in ensuring that the activities to be performed by that staff or contractor comply with the Surveillance Ordinance and this Policy.

III. Use of Surveillance Technology in Exigent Circumstances

The Police Department may temporarily acquire or use Surveillance Technology in Exigent Circumstances, provided that any such acquisition or use is reported within 90 days following the end of those Exigent Circumstances (unless the 90-day deadline is extended) and is described in the next Annual Surveillance Report submitted to the City Council pursuant to Section 10.63(c) of the Ordinance following the end of those Exigent Circumstances. The Chief of Police may, pursuant to Section 10.63(c)(3), redact any public documents submitted under this Ordinance to the extent required to comply with an order by a court of competent jurisdiction, or to exclude information that, in the reasonable discretion of the Chief of Police, if disclosed, would materially jeopardize an ongoing investigation or otherwise represent a significant risk to public safety and security provided, however, that any information redacted pursuant to this paragraph will be released in the next annual surveillance report following the point at which the reason for such redaction no longer exists.

IV. Amendments.

This Policy may be amended from time to time by the Mayor, provided that any proposed amendment shall be submitted to the City Council for approval.

APPENDIX A: SURVEILLANCE TECHNOLOGY IMPACT REPORT

Division or Unit (if applicable):	
Compliance Officer:	
Submitted by:	
Date:	
Surveillance Technology:	

1. How does the proposed Surveillance Technology will work? How does it collect Surveillance Data.

2. What is the proposed purpose of the Surveillance Technology?

3. What type of surveillance will the surveillance technology conduct? What type of surveillance data will be gathered?

4. Where will the Surveillance Technology be deployed? When?

5. What are the impacts or potential impacts on privacy, civil rights, and civil liberties in the city for individuals, communities, or groups (including, but not limited to, communities of color or other marginalized communities)? Is there a plan to address these potential impacts? If yes, describe the plan.

6. What are the estimated fiscal costs of the Surveillance Technology, including initial costs, ongoing maintenance and personnel costs, and source of funds?

7. How does the surveillance use policy apply to this surveillance technology? If it is not applicable, you must submit a technology-specific surveillance use policy.

APPENDIX B: CITY OF SOMERVILLE ANNUAL SURVEILLANCE REPORT

Division or Unit (if applicable):	
Compliance Officer:	
Submitted by:	
Date:	
Surveillance Technology:	

1. What Surveillance Technologies has the department used in the last year? Describe how the surveillance technology was used, and whether it captured images, sound, or information regarding members of the public who were not suspected of engaging in unlawful conduct.

2. Has any Surveillance Technology data been shared with a third-party?

3. What complaints (if any) has your department received about Surveillance Technology?

4. Were any violations of the Surveillance Use Policy found in the last year?

5. Has Surveillance Technology been effective in achieving its identified purpose?

6. Did the department receive any public records requests concerning Surveillance Technology? If so, how many requests?

7. How much did it cost to acquire and operate Surveillance Technology? Estimate the total annual cost of acquiring and operating the technology (e.g. equipment costs, licensing fees). What sources of funding will fund the technology in the coming year, if known.

8. Are any communities disproportionately impacted by Surveillance Technology?

9. Did your department enter into any new agreements in the past 12 months with non-city entities that included acquiring, sharing, or otherwise using surveillance technology or surveillance data?

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):	
Compliance Officer:	
Submitted by:	
Date:	
Surveillance Technology:	

1. What is the purpose of the Surveillance Technology?

2. What are the authorized uses of the Surveillance Technology? Are there any restrictions on those uses?

3. What Surveillance Data is collected by the Surveillance Technology?

4. Who can access the Surveillance Data? What is the process by which those individuals will be authorized to access the Surveillance Data?

5. How will Surveillance Data be protected?

6. For how long will Surveillance Data be retained?

7. What Surveillance Data may be accessed by the public?

8. Will any Surveillance Data be shared with third-parties? If so, why? What restrictions will be placed on the recipient of the Surveillance Data?

9. What training will any users of the Surveillance Technology receive?

10. Who is responsible for overseeing the use of the Surveillance Technology and the Surveillance Data collected? How will this person conduct oversight?