City of Cambridge
Surveillance Use Policy

This Surveillance Use Policy (the "Policy") is issued on _____(the "Effective Date") by the City Manager for the City of Cambridge (the "City") pursuant to Chapter 2.128, Section 2.128.050 of the Cambridge Municipal Code (the "Ordinance"). The Ordinance provides for the regulation of the City's use or acquisition of Surveillance Technology as defined in Section 2.128.020(G) of the Ordinance and for the collection, use, and retention of Surveillance Data as defined in Section 2.125.020(E) 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.

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. Permissible Purposes and Authorized Uses for Surveillance Technology in Departments Other than the Police Department.

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

A. Identifying and preventing threats to persons and property and preventing injury to persons or significant damage to property;
B. Identifying, apprehending, and prosecuting criminal offenders;
C. Gathering evidence of violations of any law in criminal, civil, and administrative proceedings;
D. Providing information to emergency personnel;
E. Documenting and improving performance of City employees;

F. Executing financial transactions between the City and any individual engaged in a financial transaction with the City;
G. Preventing waste, fraud, and abuse of City resources;
H. Maintaining the safety and security of City employees, students, customers, and City-owned or controlled buildings and property;
I. Enforcing obligations to the City;
J. Operating vehicles for City business;
K. Analyzing and managing service delivery;
L. Communicating among City employees, with citizens, or with third parties; and
M. Surveying and gathering feedback from constituents.

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

III. Permissible Purposes and Uses for Surveillance Technology in the Police Department.

Other than the explicit exceptions or exemptions in the Ordinance and as referenced in this Section III, the Police Department shall be subject to all City policies regarding Surveillance Technology and Surveillance Data, including this Policy.

A. The Police Department may acquire, share, or otherwise use Surveillance Data from or with a non-City entity without prior approval from the City Council, pursuant to Ordinance Section 2.128.030(B)(4).

B. 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 2.128.040 of the Ordinance following the end of those Exigent Circumstances.

C. The Police Commissioner may, pursuant to Section 2.128.070(B)(1) of the Ordinance, withhold information regarding a particular Surveillance Technology being used pursuant to a warrant where: (a) the City is prohibited from publicly releasing information pertaining to the surveillance under federal or state law, or pursuant to a Court Order; or (b) the Police Commissioner determines that release of detailed information about the present use of the Surveillance Technology would compromise public safety and security, provided that the information is released in the next Annual Surveillance Report following the Police Commissioner's determination that public safety and security concerns pertaining to the release of such information no longer exist.

IV. 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 City Manager 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.

A. 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.

In accordance with the Ordinance, the City has reviewed all of the Surveillance Technology currently in use by City departments as of the Effective Date. The Surveillance Technology, the departments that use or propose to acquire or use the Surveillance Technology, 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, shall be submitted in a report to the City Manager by each Department Head for each City department which uses or proposes to use Surveillance Technology. 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 City Manager, 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 City Manager, the City Solicitor, or the Personnel Director.

B. 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 the Information Technology Department ("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 City Manager and the City Solicitor, and propose additional measures to protect Surveillance Data from inadvertent or unauthorized disclosure.

C. 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 ITD, the City Manager 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.

D. 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:

1. 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

2. A Department Head may seek an exception for a particular type of Surveillance Data from the City Manager on a case-by-case basis.

All exceptions and the reasons therefor shall be included in a department's Annual Surveillance Report.

V. 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*.), Chapter 2.126 of the Cambridge Municipal Code (the "Open Data Ordinance"), 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 2.128.020(C) 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 City Manager 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 IV(C) above, and may only be distributed to third parties in accordance with this Section V of this Policy. However, any department may share Surveillance Data with the Police Department under Exigent Circumstances.

VI. 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.

VII. Relationship to Other Policies and Required Reports.

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. Departments Heads shall be responsible for submitting to the City Manager the following documents required by the Ordinance:

A. Surveillance Technology Impact Report(s) (Section 2.128.030) in the form provided in Appendix B attached hereto—submitted for each proposed acquisition or use of Surveillance Technology.

B. Annual Surveillance Report(s) (Section 2.128.060) in the form provided in Appendix C attached hereto—submitted annually by the City Manager 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 on December 10, 2019. Thereafter, the report will be due to the City Council by March 1 of each year.

C. Technology-Specific Surveillance Use Policy(ies) (Section 2.128.030) in the form provided in Appendix D attached hereto—submitted for each proposed acquisition or use of Surveillance Technology not already covered under this Policy.

When providing any of the above reports or a Technology-Specific Surveillance Use Policy, 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.

VIII. Amendments.

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

Approved by:

_____ Date: _____

Louis A. DePasquale
City Manager

APPENDIX A: FORM FOR INTERNAL REPORT TO CITY SOLICITOR OF TECHNOLOGY THAT MAY BE SURVEILLANCE TECHNOLGY

Department	
Unit or Division	
Compliance Officer	
Surveillance Technology (Software & Application	
What is the purpose of your Department's use or proposed use of this Surveillance Technology?	
What Surveillance Data does the Department collect with this Surveillance Technology?	
Is the Surveillance Data collected the minimum amount of data that can be collected to fulfill the purpose for which the Department uses the Surveillance Technology?	
Explanation as to why more than the minimum Surveillance Data is collected (if applicable)	
Who in your Department has access to this Surveillance Data?	
How do you protect the Surveillance Data from unauthorized access?	
How long is the Surveillance Data retained?	
Can the public access this Surveillance Data?	
How and why the public has access (if applicable)	
Is this Surveillance Data shared with third parties (e.g., state or federal agencies, contractors)?	
How and why Surveillance Data is shared with third parties, including restrictions (if applicable)	
What training will users of the Surveillance Technology receive?	

APPENDIX B: SURVEILLANCE TECHNOLOGY IMPACT REPORT

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

1. **Describe how the proposed Surveillance Technology will work, including how it will collect Surveillance Data.**

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

3. **Where will the Surveillance Technology be deployed? When?**

4. **What privacy impact will the Surveillance Technology have?**

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

APPENDIX C: CITY OF CAMBRIDGE ANNUAL SURVEILLANCE REPORT

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

1. **What Surveillance Technologies has the department used in the last year?**
   List each Surveillance Technology and, for each Surveillance Technology, describe how it works and what it has been used for. For example: "Automatic license plate readers. Deployed on police and traffic enforcement vehicles to read license plates of vehicles as selected by the individual operator. Used by traffic enforcement to enforce parking laws. Used by police to aid in the identification and recovery of stolen vehicles."

2. **Has any Surveillance Technology data been shared with a third-party?**
   List each entity with which Surveillance Data was shared, the date(s) on which Surveillance Data was shared with each entity, the type of Surveillance Data shared, and the purpose for sharing.

3. **What complaints (if any) has your department received about Surveillance Technology?**
   Describe how many complaints were received, the subject of the complaints, any department response, and the organizations responsible for the complaints, if any.

4. **Were any violations of the Surveillance Use Policy found in the last year?**
   List all known violations, the department's diagnosis of the reason for the violation, and what remedial action was taken by the department. Also, identify steps taken to determine if violations have occurred.

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

For each Surveillance Technology and each stated purpose listed in (1) above, describe whether the Surveillance Technology has been effective in realizing the purpose. Be specific, using

quantitative data whenever possible. For example: “Automatic license plate readers. Identified 800 vehicles that had exceeded posted parking time limits, leading to $40,000 in fines collected.”

6. **Did the department receive any public records requests concerning Surveillance Technology?**
   Describe how many requests were received, how many records the department produced in response thereto, and generally what information the requests were seeking.

7. **How much did it cost to acquire and operate Surveillance Technology?**
   For each Surveillance Technology listed in (1) above, list all costs associated therewith. Costs include but are not limited to operating personnel, maintenance, upgrades, training, storage, and acquisition. Also explain the source of funding for each Surveillance Technology for next year.

8. **Are any communities disproportionately impacted by Surveillance Technology?**
   For each Surveillance Technology listed in (1) above, explain whether and how any communities are disproportionately impacted by the use of the Surveillance Technology. “Impact” in this context may mean that a population is disproportionately the target of a Surveillance Technology, disproportionately penalized as a result of the City’s use of a Surveillance Technology, or disproportionately excluded from reaping the benefits of the City’s use of a Surveillance Technology.

   Pay particular attention to low-income communities, communities of color, or any community that is marginalized in the City. If any disproportionality exists, explain either the department’s proposed remedy or why the disproportionality is appropriate. Use quantitative data whenever possible. For example: “Automatic license plate readers. Of the 1,000 vehicles stopped due to use of ALPRs, 400 were driven by African-Americans and 200 were driven by Hispanics. This is significantly disproportionate to the population of Cambridge. The department will adjust patrols in order to ensure that ALPRs are not deployed disproportionately in communities inhabited by African-American and Hispanic residents.”

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

Department:	
Division or Unit (if applicable):	
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?**

APPENDIX E: CHECKLIST FOR SURVEILLANCE TECHNOLOGY COMPLIANCE

In order to better assist departments in compliance with the Surveillance Use Policy, we have compiled the below checklist for department heads and compliance officers to review.

1. **Is this a Surveillance Technology for which City Council approval has previously been obtained?**

    a. If yes, skip to No. 2.

    b. If no, you will need to complete the following:

        i. Surveillance Technology Impact Report (see Appendix B); and

        ii. If the Surveillance Technology is not covered in the Surveillance Use Policy, you'll also need a Technology-Specific Surveillance Use Policy (see Appendix D).

2. **Is there a proposal to use the Surveillance Technology for a purpose, in a manner, or in a location not previously approved by the City Council?**

    a. If no, skip to No. 3.

    b. If yes, you will need to resubmit a Surveillance Technology Impact Report (see Appendix B); then you will need to list the Surveillance Technology in the Annual Surveillance Report (see Appendix C) referenced below in No. 3.

3. **Surveillance Technologies previously approved by the City Council must be listed on the Annual Surveillance Report (see Appendix C) submitted to the City Council by the City Manager each year by March 1. Draft submissions for the Annual Surveillance Report must be submitted by Department Heads to the City Manager no later than January 1 of each year.**