CITY OF BOSTON

IN CITY COUNCIL

WHEREAS, Governments around the world are responding to the COVID-19 pandemic with an unprecedented use of surveillance tools, despite public health and privacy experts agreeing that public trust is essential to an effective response to the pandemic; *and*

WHEREAS, Surveillance technology and electronic data gathering can be useful tools for advancing effective delivery and analysis of constituent services, public safety and security; *and*

WHEREAS, Usage of surveillance technology must include safeguards with accountability to the public in order to protect privacy rights and civil liberties; *and*

WHEREAS, Boston Public Schools should be welcoming and safe environments for all students regardless of immigration status or race. Due to COVID-19, Boston Public Schools has transitioned entirely to online learning where it is expected that even after returning to in-person learning, technology will be a larger part of education; *and*

WHEREAS, As people in Boston and across the state are sheltering in place, we are growing more dependent on technology to connect us to each other and to our government; *and*

WHEREAS, Cities around the country such as Cambridge, Somerville, Santa Clara, and Providence have created ordinances governing the acquisition and use of surveillance technology and electronic data in order to protect the civil liberties of their citizens while allowing for appropriate use to assist in the charge of improving delivery of services and public safety; *and*

WHEREAS, As more municipalities move toward electronic data collection used to manage assets and resources efficiently and new technologies are becoming available, the public would benefit from proactive discussion of current practices and future acquisitions. *NOW, therefore be it ordained by the City Council of Boston as follows:*

That the City of Boston Code, Ordinances, be amended in Chapter XVI by adding the following after 16-62:

16-63: ORDINANCE ON SURVEILLANCE OVERSIGHT AND INFORMATION SHARING

16-63.1 Purpose: The purpose of this ordinance is to provide accountability, transparency, and oversight regarding the acquisition and use of Surveillance Technology and Surveillance Data by the City of Boston and its agencies and officers, and to protect privacy, civil rights, and racial and immigrant justice while allowing for appropriate use to assist in the charge of improving delivery of services and public safety.

16-63.2 Definitions:

The following definitions apply to this Ordinance:

> *Annual Surveillance Report* means a written report submitted by the Mayor's office on an annual basis concerning specific Surveillance Technology used during the previous year and containing the information set forth in this ordinance by the following City Departments and Agencies: the Boston Police Department, the Boston Parks Department Park Rangers, Boston Public Schools, Boston Public Health Commission, Boston Housing Authority, Boston Municipal Protection Services, and the Office of Emergency Management.

> *Exigent Circumstances* means the police commissioner, the police commissioner's designee, the head of BHA's Police, or the head of the BPHC Police's good faith and reasonable belief that an emergency involving danger of death, physical injury, or significant property damage or loss, similar to those that would render it impracticable to obtain a warrant, requires the use of the Surveillance Technology or the Surveillance Data it provides. The use of Surveillance Technology in Exigent Circumstances shall not infringe upon an individual's right to peacefully protest or exercise other lawful and protected constitutional rights.

Identifiable Individual means an individual whose identity can be revealed by data, including Surveillance Data, or revealed by data when it is analyzed and/or combined with any other type of record.

Surveillance means the act of observing or analyzing the movements, behavior, or actions of Identifiable Individuals.

Surveillance Data means any electronic data collected, captured, recorded, retained, processed, intercepted, or analyzed by Surveillance Technology acquired by the City or operated at the direction of the City.

Surveillance Technology means any device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, associational, or similar information specifically associated with, or capable of being associated with, any identifiable individual or group; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software.

a) Examples of Surveillance Technology include, but are not limited to:
    1. International mobile subscriber identity (IMSI) catchers and other cell-site simulators;
    2. Automatic license plate readers;
    3. Electronic toll readers;
    4. Closed-circuit television cameras except as otherwise provided herein;
    5. Biometric Surveillance Technology, including facial, voice, iris, and gait-recognition software and databases;
    6. Mobile DNA capture technology;
    7. Gunshot detection and location hardware and services;
    8. X-ray vans;
    9. Video and audio monitoring and/or recording technology, such as surveillance cameras;
    10. Surveillance enabled or capable light bulbs or light fixtures;
    11. Tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network;
    12. Social media monitoring software;
    13. Through-the-wall radar or similar imaging technology;
    14. Passive scanners of radio networks;

15. Long-range Bluetooth and other wireless-scanning devices;
16. Thermal imaging or "forward-looking infrared" devices or cameras;
17. Electronic database systems containing Surveillance Data about Identifiable Individuals;
18. Radio-frequency identification (RFID) scanners; and
19. Software designed to integrate or analyze data from Surveillance Technology, including surveillance target tracking and predictive policing software.

Surveillance Technology Impact Report means a written report submitted by the Mayor's office with a request for approval of acquisition or use of Surveillance Technology, and which includes, at a minimum, the requirements set forth in this ordinance.

Surveillance Use Policy means a policy for the City's use of Surveillance Technology, approved by the Corporation Counsel and the Mayor's office, and submitted by the Mayor's office to and approved by the City Council. The Surveillance Use Policy shall at a minimum satisfy the requirements set forth in this ordinance.

Technology-Specific Surveillance Use Policy means a policy governing the City's use of a specific Surveillance Technology not already covered under the City's Surveillance Use Policy, approved by the Corporation Counsel and the Mayor, and submitted by the Mayor to the City Council with a Surveillance Technology Impact Report under this ordinance.

BPS means the Boston Public Schools.

BPS personnel means any employee or agent of the Boston Public Schools, excluding School Safety Specialists.

School Safety Specialists means any officials or employees that belong to the Boston Public Schools Department of Safety Services or any other security and enforcement personnel, and that may or may not be licensed by the Boston Police Department as special police officers.

BPD means the City of Boston Police Department.

Student Report means a written record that is not an educational record protected under FERPA and that is created by School Safety Specialists or by BPS personnel and that pertains to a student. Student Reports include but are not limited to School Safety Reports, BPD Form 1.1 Incident Reports, Field Interrogation and Observation Reports, Intelligence Reports, and Face Sheets. Student Reports also include informal emails, texts, and other electronic messages that describe or contain details pertaining to student activity.

Historic Student Reports mean Student Reports that they have created or produced prior to the Effective Date of this ordinance.

Serious bodily harm means bodily injury that results in permanent disfigurement, loss or impairment of a bodily function, limb or organ, or substantial risk of death.

Surveillance Oversight Advisory Board is a group comprised of five individuals, one representative to be chosen by each of the following: the president of the City Council, the Massachusetts American Civil Liberties Union, and the Boston Police Commissioner; and two representatives chosen by the Mayor, at least one of whom shall be an academic representative with expertise in technology and public policy issues. The Board shall serve as an advisory body to host further discussion and provide recommendations on surveillance issues to the Mayor.

16-63.3 Community Control Over Surveillance

a) Applicability

This section shall ~~only~~ apply to the following City departments and agencies: the Boston Police Department, Boston Public Schools, Boston Public Health Commission, the Boston Parks Department Park Rangers, Boston Housing Authority, Boston Municipal Protection Services, and the Office of Emergency Management.

For the purpose of this section, the word “City” shall mean the City departments and agencies listed above.

b) Exceptions and Exemptions

The following situations are exceptions and exemptions from this ordinance.

1. The following do not constitute Surveillance Data and are exempted from the requirements of this Ordinance:
    A) Surveillance Data acquired where the individual knowingly and voluntarily consented to provide the information, such as submitting personal information for the receipt of City services; and
    B) Surveillance Data acquired where the individual was presented with a clear and conspicuous opportunity to opt-out of providing the information.
2. Surveillance Technology does not include the following devices, software, or hardware, which are exempt from the requirements of this ordinance, unless the devices, hardware, or software are modified to include additional surveillance capabilities:
    A) Routine office hardware, such as televisions, computers, and printers, that are in widespread public use and will not be used for any surveillance or surveillance- related functions;
    B) Parking ticket devices (PTDs) and related databases;
    C) Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously, that are used for non-law enforcement and non-investigatory purposes, and whose functionality is used for manually capturing and manually downloading video and/or audio recordings;
    D) Cameras installed in or on a police vehicle;
    E) Cameras installed pursuant to state law authorization in or on any vehicle or along a public right-of-way solely to record traffic violations or traffic patterns, provided that the Surveillance Data gathered is used only for that purpose;
    F) Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
    G) City databases that do not and will not contain any Surveillance Data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by Surveillance Technology;
    H) Manually-operated technological devices that are used primarily for internal City communications and are not designed to surreptitiously collect Surveillance Data, such as radios and email systems;

I) Parking access and revenue control systems, including proximity card readers and transponder readers at City-owned or controlled parking garages;
J) Card readers and key fobs used by City employees and other authorized persons for access to City-owned or controlled buildings and property;
K) Cameras installed on City property solely for security purposes, including closed-circuit television cameras installed by the City, to monitor entryways and outdoor areas of City-owned or controlled buildings and property for the purpose of controlling access, maintaining the safety of City employees and visitors to City buildings, and protecting City property;
L) Security cameras including closed-circuit television cameras installed by the City to monitor cashiers' windows and other cash-handling operations and to maintain the safety of City employees and visitors to such areas;
M) Cameras installed solely to protect the physical integrity of City infrastructure; or
N) Technology that monitors only City employees in response to complaints of wrongdoing or in order to prevent waste, fraud, or abuse of City resources.
O) Devices exclusively capable of detecting radiation.
P) Radio-frequency identification scanners (RFIDs) used for disaster patient tracking by the Boston Public Health Commission.
Q) BPHC technology used to track BPHC owned or leased equipment and vehicles

3. Notwithstanding the provisions of this ordinance, BPD, BHA Police, or BPHC Police may temporarily acquire or temporarily use Surveillance Technology in Exigent Circumstances for a period not to exceed 30 days without following the provisions of this chapter before that acquisition or use. However, if these bodies acquire or use Surveillance Technology in Exigent Circumstances under this section, the BPD Commissioner, BHA Head of Police, or BPHC Head of Police must:
    A) Report that acquisition or use to the City Council in writing within 30 days following the end of those Exigent Circumstances;
    B) Submit a Surveillance Technology Impact Report, and, if necessary, a technology-specific Surveillance Use Policy to the City Council regarding that Surveillance Technology within 30 days following the end of those Exigent Circumstances; and

C) Include that Surveillance Technology in the Department or Agency's next Annual Surveillance Report to the City Council following the end of those Exigent Circumstances.

D) If the Department or Agency is unable to meet the 30-day timeline to submit a Surveillance Technology Impact Report and, if necessary, a technology-specific Surveillance Use Policy to the City Council, the Department or Agency must notify the City Council in writing requesting to extend this period. The City Council may grant extensions beyond the original 30-day timeline to submit a Surveillance Technology Impact Report, and, if necessary, a technology-specific Surveillance Use Policy.

E) Any Surveillance Technology Impact Report, and, if necessary, any Technology-Specific Surveillance Use Policy submitted to the City Council under this subsection shall be made publicly available on the City's website upon submission to the City Council.

F) Any Surveillance Technology Impact Report and, if necessary, technology-specific Surveillance Use Policy submitted to the City Council under this section may be redacted 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 Commissioner 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.

4. A City department head may apply a technical patch or upgrade that is necessary to mitigate threats to the City's environment. The department shall not use the new surveillance capabilities of the technology until the requirements of this ordinance are met, unless the Mayor, or their designee, determines that the use is unavoidable; in that case, the Mayor shall request City Council approval as soon as possible. The request shall include a report to the City Council of how the altered surveillance capabilities were used since the time of the upgrade. If the City Council does not approve the use of the proposed new surveillance capabilities, the request shall be sent to the Surveillance Oversight Advisory Board who will make recommendations to the Mayor. Subsequent to receiving the recommendations from the Surveillance Oversight Advisory Board, the Mayor may at their discretion resubmit a modified request to the City Council for approval.

c) Surveillance Use Policy

1. The Mayor shall submit to the City Council for its review and approval a proposed Surveillance Use Policy applicable to each applicable City Department that possesses or uses Surveillance Technology before the effective date of this ordinance. If the City Council does not approve the use of the proposed new surveillance capabilities, the request shall be sent to the Surveillance Oversight Advisory Board who will make recommendations to the Mayor. Subsequent to receiving the recommendations from the Surveillance Oversight Advisory Board, the Mayor may at their discretion resubmit a modified request to the City Council for approval.
2. Any Surveillance Use Policy submitted under this section shall be made publicly available upon submission to the City Council.
3. A Surveillance Use Policy shall at a minimum specify the following:
    A) Purpose: the specific purpose(s) for the Surveillance Technology;
    B) Authorized use: the uses that are authorized, the rules and processes required before that use, and the uses that are prohibited;
    C) Data collection: the Surveillance Data that can be collected by the Surveillance Technology;
    D) Data access: the individuals who can access or use the collected Surveillance Data, and the rules and processes required before access or use of the information;
    E) Data protection: the safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms;
    F) Data retention: the time period, if any, for which information collected by the Surveillance Technology will be routinely retained, the reason that retention period 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;
    G) Public access: if and how collected Surveillance Data can be accessed by members of the public, including criminal defendants;
    H) Information and data-sharing: if and how other City or non-City entities can access or use the Surveillance Data, how information is shared among City agencies or between City agencies and non-City entities and organizations, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the Surveillance Data;

I) Training: the training, if any, required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology, including whether there are training materials;
J) 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, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy;
K) Legal Authority: the statutes, regulations, or legal precedents, if any, that control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology; and
L) Child Rights: special considerations specific to Surveillance Technology and Surveillance Data pertaining to minor children.

4. The City Council shall vote to approve or deny the Surveillance Use Policy by a vote of a simple majority within 60 days of submission. If the City Council does not approve the Surveillance Use Policy, the Policy shall be sent to the Surveillance Oversight Advisory Board who will make recommendations of improvement to the Mayor. Subsequent to receiving the recommendations from the Surveillance Oversight Advisory Board, the Mayor may at their discretion resubmit a modified request to the City Council for approval.

d) Surveillance Technology Impact Report and Technology-Specific Surveillance Use Policy

1. The Mayor's office must seek and obtain approval from the City Council as set forth in this section prior to the City acquiring, using, or entering into an agreement to acquire, share or otherwise use, unapproved Surveillance Technology or Surveillance Data as defined in this ordinance.

A) The City may seek, but not accept, funds for Surveillance Technology without approval from the City Council, provided that the City shall notify the City Council of the funding application at the time it is submitted, and include in this notification the deadline of the funding opportunity and details regarding the nature of the Surveillance Technology for which funding is sought. If the City Council declines to accept funds for Surveillance Technology the request to accept the funds shall be sent to the Surveillance Oversight Advisory Board who will make recommendations to the Mayor. Subsequent to receiving the recommendations from the Surveillance Oversight Advisory Board, the Mayor may at their discretion resubmit a modified request to the City Council for approval.

2. Acquisition of Surveillance Technology by applicable City departments. Unless exempted or excepted from the requirements of this ordinance, any applicable City department intending to acquire new Surveillance Technology or Surveillance Data, including but not limited to procuring that Surveillance Technology without the exchange of monies or other consideration, or use Surveillance Technology or Surveillance Data for a purpose or in a manner not previously approved, shall, prior to acquisition or use, obtain council approval of the acquisition or use. The process for obtaining approval shall be as follows:
    A) The City department shall submit a Surveillance Technology Impact Report, and, if necessary, a Technology-Specific Surveillance Use Policy, as described below, to the Mayor's office for review and approval.
    B) If the request is approved by the Mayor's office, the Mayor's office shall submit the request, including copies of the City department's Surveillance Technology Impact Report and, if applicable, Technology-Specific Surveillance Use Policy, to the City Council for review.
    C) The City Council shall have 60 days from the date of submission to approve or deny a request by majority vote for the acquisition or use of Surveillance Technology. If the City Council does not approve the acquisition or use of Surveillance technology the request shall be sent to the Surveillance Oversight Advisory Board who will make recommendations to the Mayor. Subsequent to receiving the recommendations from the Surveillance Oversight Advisory Board, the Mayor may at their discretion resubmit a modified request to the City Council for approval.
    D) Contents of Surveillance Technology Impact Report. A Surveillance Technology Impact Report submitted shall include all of the following:
    E) Information describing the Surveillance Technology and how it works;

F) Information on the proposed purpose(s) for the Surveillance Technology;
G) Information describing the kind of surveillance the Surveillance Technology will conduct and what Surveillance Data will be gathered, including a detailed accounting of which entities may have access to any Surveillance Data, under what circumstances (e.g. ongoing automated access, subject to an informal request, subject to subpoena, subject to a warrant, etc.);
H) The location(s) the Surveillance Technology may be deployed and when;
I) A description of the privacy and anonymity rights affected and a mitigation plan describing how the department's use of the equipment will be regulated to protect privacy and anonymity, and to limit the risk of abuse;
J) The potential impact(s) on privacy in the City; the potential impact on the civil rights and liberties of any individuals, communities or groups, including, but not limited to, communities of color or other marginalized communities in the City, and a description of a plan to address these impact(s);
K) An estimate of the fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding; and
L) An explanation of how the Surveillance Use Policy will apply to this Surveillance Technology and, if it is not sufficiently applicable, a Technology-Specific Surveillance Use Policy.

3. A Technology-Specific Surveillance Use Policy shall be required if the purpose, authorized use, data collection, data access, data protection, data retention, public access, third-party data sharing, training, or oversight of the requested Surveillance Technology differ from the standards in the Surveillance Use Policy submitted under Sections 16-63.3c and 16-63.3d.
   A) A Technology-Specific Surveillance Use Policy shall not conflict with any provision of the City's Surveillance Use Policy.
   B) To the extent a conflict arises between the provisions of the City's Surveillance Use Policy and a Technology-Specific Surveillance Use Policy, the City's Surveillance Use Policy shall govern. A Technology-Specific Surveillance Use Policy shall include all of the elements of the Surveillance Use Policy as outlined in Section 16-63.3b.

~~4.~~ Any Surveillance Technology Impact Report, and, if necessary, Technology-Specific Surveillance Use Policy submitted to the City Council under Sections 16-63.3c and 16-63.3d shall be made publicly available on the City's website upon submission to the council.

16-63.4 Boston Public Schools And Boston Police Department Information-sharing Policy

a) School Safety Specialists shall not collect, store, or share information pertaining to students except by creating and sharing Student Reports in accordance with this Chapter.
    1. Student Reports shall only be created when:
        A) Serious bodily harm to an individual has occurred as a result of willful conduct by a student;
        B) A credible threat to the safety of the school arises that would amount to criminal conduct;
        C) A student is in possession of firearms as defined in Chapter 269 section 10 (j), ammunition, or a dangerous weapon as defined in M.G.L. Chapter 269 section 10 (b); or
        D) A student unlawfully possesses or uses controlled substances, provided those substances are not marijuana, nicotine, or alcohol, and further provided, however, that School Safety Specialists may collect, store and share information pertaining to unlawful distribution of alcohol or marijuana when a student has unlawfully distributed marijuana or alcohol on school grounds in excess of the following amounts: thirty (30) grams for marijuana and one (1) liter for alcohol.
    2. School Safety Specialists may not create a Student Report relating to matters that are not described above.
    3. Student Reports shall not contain information pertaining to:
        A) Immigration status;
        B) Citizenship;
        C) Address and/or neighborhood of residence;
        D) Religion;
        E) National origin;
        F) Students' native or spoken language;
        G) Suspected, alleged, or confirmed gang involvement, affiliation, association, or membership;
        H) Participation in school activities, extracurricular activities outside of school, sports teams, or school clubs or organizations;
        I) Degrees, Honors, or Awards; or
        J) Post-high school plans.

4. Before creating the Student Report, the School Safety Specialists must discuss the writing of the report with the Principal(s) or Head(s) of School of (i) the school(s) where the subject(s) of the report is/are enrolled and (ii) the school where the School Safety Specialists writing the report is assigned to work. The required Principals or Heads of School must document in writing that the incident at hand merits a report under the criteria in Section 16-63.4a.
5. Principals and Heads of School of (i) the school(s) where the subject(s) of the report is/are enrolled and (ii) the school where the School Safety Specialists writing the report is assigned to work must receive copies of all Student Reports written under this section immediately upon writing.
    A) Within 24 hours of the writing of a Student Report under this section, the relevant Principals and/or Heads of School must provide a copy of the report, with any necessary redactions to protect student privacy, to every student referenced by name in the Report, as well as to those students' families. Reports which involve allegations of parental/household abuse may also be withheld from students' families if disclosure of the report is not in the best interest of the student. In cases of allegations of parental/household abuse, a copy of the Report shall be provided to the student or a trusted adult of their choosing.

b) Rules for Student Information Sharing
    1. School Safety Specialists and BPS personnel shall not transmit to or share with BPD or any other outside entities any information about students, including but not limited to Student Reports, through any official or unofficial channels, including but not limited to text, phone, email, database, and in-person communication, except if the transmission or sharing is done (i) pursuant to Section 16-63.4c or (ii) in Exigent Circumstances pursuant to Section 16-63.4d.

c) Transmitting information to the BPD and other entities outside the Boston Public Schools
    1. BPS personnel and School Safety Specialists may not send information relating to Boston Public Schools students to the Boston Regional Intelligence Center (BRIC), federal immigration authorities, federal law enforcement agencies, or any law enforcement fusion center under any circumstances, except where required by state or federal law.
    2. BPS personnel may not transmit to the BPD any student information, including but not limited to a Student Report, unless in response to a judicial warrant issued upon a finding of probable cause, as required under MGL c. 269, sec. 10(j) and MGL c. 71, sec. 37L, or as otherwise required by state or federal law. Nothing in this ordinance shall limit the ability of Boston Public Schools to release information as required by state or federal laws and regulations.

3. Before BPS personnel or a School Safety Specialists transmits a Student Report created pursuant to Section 16-63.4a or any other information relating to a student to BPD or to any other entity outside of the Boston Public Schools in accordance with Sections 16-63.4c1 and 16-63.4c2, the following must take place:
    A) Any student named in a Student Report or other record, and their parent or guardian, must be notified in writing that the Student Report they received pursuant to Section 16-63.4a5A will be transmitted to BPD or to the outside agency and receive an explanation of why the information reflected in the report is prompting the communication. All written materials must be provided in both English and the language spoken by the relevant student's parent or guardian.
    B) The Boston Public Schools must schedule a meeting with the student and the student's parent or guardian as soon as practicable, and an interpreter of the family's choosing must be present for any party that requires one. The interpreter cannot be the student or other individual who is participating in the meeting in another capacity. If the family does not have a preferred interpreter, BPS must provide a qualified translator.
    C) The Principals and Heads of School mentioned in Section 16-63.4a5A, the Superintendent, and the Legal Advisor for the School Department must review the Student Report and the Legal Advisor for BPS must verify that at least one of the criteria in Section 16-63.4a1 is present. If the Legal Advisor finds that the incident did not meet the criteria in Section 16-63.4a1, they must place a note in the record attesting to this fact, and the Student Report may not be transmitted to the BPD or any entity outside of BPS.
    D) The student and family may have an attorney and/or advocate present at the meeting. At the moment the meeting is scheduled and requested, BPS must provide the family with a list of available legal services vetted by the Mayor's Office of Immigrant Advancement.
    E) Students and families may amend a student's record by placing a note with information relating to any Student Report in which the student is named in the student's file.

d) Transmission of information pursuant to Exigent Circumstances
    1. Within 12 hours after a School Safety Specialists transmits a Student Report created pursuant to Section 16-63.4a or any other information relating to a student to the BPD pursuant to the existence of Exigent Circumstances:

A) The School Safety Specialists must notify the relevant Principal or Head of School that student information was shared with the BPD, and provide the relevant Principal or Head of School with a copy of the information shared;

2. Within 24 hours after the conclusion of the exigent circumstance or within 24 hours after BPS Personnel or a School Safety Specialists transmits a Student Report created pursuant to Section 16-63.4a or any other information relating to a student to the BPD pursuant to the existence of Exigent Circumstances, the relevant Principal or Head of School shall:
    A) Notify in writing any student whose information or Student Report was shared and their parent or guardian that the student information was shared, and share a copy of the information transmitted and an explanation of the incident prompting the communication to BPD after the information was transmitted. All written materials must be provided in both English and the language spoken by the parent or guardian.
    B) The relevant Principal or Head of School must schedule a meeting with the student and the student's parent or guardian as soon as practicable, and an interpreter/translator of the parent or guardian's choosing must be present for any party that requires one. The interpreter/translator cannot be the student or other individual who is participating in the meeting in another capacity. If the family does not have a preferred translator, BPS must provide a qualified translator.
        I. The student and parent or guardian may have an attorney and/or advocate present at the meeting. At the moment the meeting is scheduled and requested, BPS must provide the family with a list of available legal services vetted by the Mayor's Office of Immigrant Advancement.
    C) If the information shared was a Student Report, the Principals and/or Heads of School mentioned in Section 16-63.4a5, the Superintendent, and the Legal Advisor for the School Department must review the Student Report and the Legal Advisor for BPS must verify that at least one of the criteria in Section 16-63.4a1 is present. If the Legal Advisor finds that the incident did not meet the criteria in Section 16-63.4a1 they must place a note in the record attesting to this fact, and the BPD must be notified to the same within 3 business hours.

e) School Safety Specialists shall not attend any meetings where officers or employees from U.S. Immigrations and Customs Enforcement are present, either in person or virtually.

f) Transparency and Communication

1. Students, families, school administrators, teachers, and counselors must be made aware of this ordinance by including a copy of the ordinance in the Guide to Boston Public Schools.

g) Community Information-Sharing Oversight Board
   1. A community oversight board shall be created to provide oversight regarding the implementation of Section 16-63.4 of this ordinance.
   2. The board must include at least one representative from each of the following groups: a student chosen by the Boston Student Advisory Council, a parent or guardian chosen by the Citywide Parent Council, a parent or guardian chosen by the Boston Special Education Parent Advisory Council, a representative chosen by the Code of Conduct Advisory Council, a representative of the District English Learner Advisory Committee, a teacher chosen by the Boston Teachers Union, a local immigration advocate chosen by the Student Immigrant Movement (SIM), a civil rights advocate chosen by Lawyers for Civil Rights, and an immigration attorney familiar with the immigration consequences of criminal proceedings chosen by the Political Asylum/Immigration Representation Project.
   3. The Superintendent shall report monthly to the board:
      A) The number of Student Reports created, disaggregated by school;
      B) The number of Student Reports shared with any outside entity, disaggregated by school and receiving entity;
      C) The number of Student Reports reviewed by the Legal Advisor for the School Department that did not meet the criteria specified in Section 16-63.4a1, disaggregated by school, and including the date of each incident, a description of each incident, the race, ethnicity, gender, age, and grade level of each student who is named in the report, the location of the incident, and whether the report was transmitted to BPD or to any other outside entity.
      D) The number of Student Reports written under Section 16-63.4a, disaggregated by school, including the date of the incident, a description of the incident including the justification for the creation of the report per Section 16-63.4a1, the type of report, the race, ethnicity, gender, age and grade of each student who is named in the report, the location of the incident, and whether the report was transmitted to BPD or to any other outside entities.
   4. The board will review the information provided under Section 16-63.4g3 and may request that School Safety Specialists or District personnel respond to questions, either in writing or at a public meeting, relating to the information provided.

5. The board shall review the information for patterns and compliance with this ordinance. It shall issue findings and report such findings to the City Council and School Committee on a quarterly basis.

h) Accountability and Training
    1. All School Safety Specialists and school administrators must receive training on this policy, and the training will be designed in collaboration with the Student Immigrant Movement and Boston Teachers Union's Unafraid Educators. The training will also be provided by the Central Office and not by individual schools. Training materials will be made publicly available.
    2. All School Safety Specialists and BPS personnel, including school administrators, will sign an acknowledgment of responsibility for safeguarding student information under Section 16-63.4 of this ordinance, FERPA, and state student records law.
    3. All new School Safety Specialists will receive training on the requirements of Section 16-63.4 of this ordinance as part of their orientation.
    4. All School Safety Specialists must be trained every three years or at the discretion of the community oversight board.
    5. Any transfer of information about students in violation of Section 16-63.4 of this ordinance shall result in appropriate disciplinary action, up to and including dismissal, in accordance with the rules of collective bargaining.
    6. Should any School Safety Specialist be found to have violated this policy, the Superintendent will instruct the Chief of Safety Services to suspend all authorization of School Safety Specialists report submissions to BPD pending a full investigation of such violation.
i) Nothing in this section shall be construed to prevent or restrict reporting requirements around sexual assault, sexual abuse, and child abuse in accordance with Massachusetts General Laws.

16-63.5 Annual Surveillance Report

a) Applicability: This section shall apply to the following City departments and agencies: the Boston Police Department, Boston Parks Department Park Rangers, Boston Public Schools, Boston Public Health Commission, Boston Housing Authority, Boston Municipal Protection Services, and the Office of Emergency Management.

    For the purpose of this section, the word "City" shall mean the City departments and agencies listed above.

b) Within 18 months of the effective date, and annually thereafter, all applicable City departments shall submit to the Mayor an Annual Surveillance Report pertaining to each City department for which approval for the use of Surveillance Technology or Surveillance Data has been obtained under Sections 16-63.3c and 16-63.3d of this ordinance. Upon receipt of such reports, the Mayor shall promptly submit them to the City Council. Any Annual Surveillance Report submitted under this section shall be made publicly available on the City's website upon submission to the council.

c) The Annual Surveillance Report submitted pursuant to this section shall include all of the following:

    1. A description of how Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct;
    2. Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal, the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure;
    3. A summary of community complaints or concerns about the Surveillance Technology, if any;
    4. The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City;
    5. A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose;
    6. The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year;
    7. An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known;
    8. Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City are disproportionately impacted by the deployment of the Surveillance Technology; and
    9. A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using Surveillance Technology or the Surveillance Data it provides.

d) Based upon information provided in the Annual Surveillance Report, the City Council shall determine whether the benefits to the applicable, impacted City department(s) and the community of the Surveillance Technology outweigh the financial and operational costs and whether reasonable safeguards exist to address reasonable concerns regarding privacy, civil liberties, and civil rights impacted by the deployment of the Surveillance Technology. If the benefits or reasonably anticipated benefits do not outweigh the financial and/or operational costs or civil liberties or civil rights are not reasonably safeguarded, the City Council may recommend modifications to the Surveillance Use Policy that are designed to address the City Council's concerns to the Mayor for their consideration; withdraw authorization for continued use of Surveillance Technology by a majority vote of the City Council; and/or request a report back from the Mayor regarding steps taken to address the City Council's concerns. Should the Council withdraw authorization for a previously approved surveillance technology, the Mayor may request that the Surveillance Oversight Advisory Board meet to discuss the City Council's concerns and provide recommendations to the Mayor. The mayor at their discretion may resubmit a modified request to the City Council for approval.
e) Nothing in this ordinance shall prohibit the City Council from enacting a separate ordinance to ban or otherwise regulate any Surveillance Technology, whether previously approved or not.
f) No later than May 31 of each year, the City Council shall hold a meeting to discuss the applicable City departments' Annual Surveillance Reports, and shall publicly release a report that includes a summary of all requests for approval of Surveillance Technology received by the City Council during the prior year, including whether the City Council approved or denied the City's request for acquisition or use of the Surveillance Technology.

16-63.6 Enforcement

a) Enforcement officials: This ordinance shall be enforced by the Mayor's office or the Mayor's designee.
b) Suppression: No data collected or derived from any use of Surveillance Technology in violation of this ordinance and no evidence derived therefrom may be received in evidence in any proceeding in or before any department, officer, agency, regulatory body, legislative committee, or other authority subject to the jurisdiction of the City of Boston.

c) Cause of action: Any violation of this ordinance constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this ordinance. An action instituted under this paragraph shall be brought against the City and, if necessary to effectuate compliance with this ordinance, any other governmental agency with possession, custody, or control of data subject to this ordinance.
d) The City will address alleged violations of this ordinance in accordance with its usual practices, applicable law, and contractual obligations.
e) Whistleblower protections. Subject to the limitations and requirements set forth in G. L. c. 149, §185 (the "Massachusetts Whistleblower Statute" or "Section 185") as it may be amended from time to time, any City employee as defined in Section 185 who reports an alleged violation of this ordinance, shall be afforded protections against retaliation if applicable pursuant to Section 185, as set forth in and subject to the limitations and requirements of Section 185.
f) Nothing in this ordinance shall be construed to limit or affect any individual's rights under state or federal laws.

16-63.7 Severability

a) The provisions in this ordinance are severable. If any part or provision of this ordinance, or the application of this ordinance to any person or circumstance, is held invalid by a court of competent jurisdiction, the remainder of this ordinance shall not be affected by such holding and shall continue to have full force and effect.

16-63.8 Effective Date and Implementation

The effective date and implementation of the ordinance shall be as follows.

a) The ordinance shall take effect and be implemented in the manner and ways described in this section.
b) The ordinance shall take effect notwithstanding any other provision of law and shall supersede any prior law and regulation enacted by the City of Boston and/or any agreement entered into by the City of Boston or any of its agencies that are interpreted to be in conflict with its provisions.
c) Sections 16-63.1, 16-63.2, 16-63.4, 16-63.6, and 16-63.7 shall take effect one month after its adoption in accordance with the following provisions:
    1. Every School Safety Specialist shall create a record of Historic Student Reports
    2. Within four months of the Effective Date:

A) The Historic Student Reports that do not conform with Section 16-63.4a1 shall be destroyed, in both print and electronic form, provided that such destruction is permitted under the state law relating to retention of records.
B) The Historic Student Reports that conform with Section 16-63.4a1 can be retained, provided there is a previous certification by the BPS Legal Advisor that their creation meets such requirements.
C) All reports created more than 5 years ago shall be destroyed.

3. Within six months of the Effective Date, the Head of the School Safety Specialists and the Legal Advisor must submit a report to the Community Information-Sharing Oversight Board. Such report must contain:
   A) The number of Historic Student Reports, including the format or file type of the report, description of each incident, disaggregated by race, ethnicity, gender, age, and grade level of each student who is named in the report;
   B) The number of Historic Student Reports retained in accordance with Section 16-63.8c2A;
   C) The number of Historic Student Reports destroyed in accordance with Section 16-63.8c2B and 16-63.8c2C;
4. No more than one month after receiving such report, the Community Information-Sharing Oversight Board shall call a public hearing to discuss the Historic Student Reports. The Head of the School Safety Specialists as well as individual School Safety Specialists shall be present at such public hearing.

d) Sections 16-63.3 and 16-63.5 shall take effect nine months after their adoption.

16-63.9 Establishment of a Surveillance, Data, and Privacy Working Group

a) The Working Group shall be tasked with identifying a set of priorities and implementable objectives to increase the transparency, accountability, and engagement around the public deployment of technology and use of data within City of Boston Departments not covered by this ordinance.
b) The Working Group will move forward sustainable policies to increase engagement on the topic of privacy and supply recommendations on professional development opportunities and training for City staff.
c) The Working Group must produce recommendations for implementation within one year from the date of adoption to the Mayor and City Council.

d) The Working Group shall comprise a representative from the Mayor's Office of New Urban Mechanics, a representative from the Department of Innovation and Technology, a representative from the City Council to be chosen by the Boston City Council President, a representative from the Massachusetts American Civil Liberties Union, a representative from the community-at-large to be chosen by SIM, and a representative appointed by the Mayor.
e) The Working Group will dissolve upon the publication of recommendations to the Mayor and City Council.
f) The Working Group seats shall be filled within one month of this ordinance's passage and the Group shall convene for its first meeting one month thereafter.

Filed in City Council: October 20, 2021