

To: **COUNCIL**

Meeting Date: **10/19/2021**

Subject: **Video Surveillance Privacy Complaint Report MI118-5 / Privacy Impact Assessment**

Submitted By: **Danielle Manton, City Clerk**

Prepared By: **Mary Carr, Supervisor of Information Management and Archives**

Report No.: **21-176(CRS)**

File No.: **A18**

Recommendation(s)

THAT Council receive Report No. 21-176 (CRS) Video Surveillance Complaint Report MI18-5 / Privacy Impact Assessment for information; and

THAT Council approve the draft policy attached as Appendix E - Use of Corporate Cameras Policy.

Executive Summary

Purpose

- This report provides an outline of the Privacy Complaint investigation launched in 2018 by the Information Privacy Commissioner and provides an overview of the recommendations in the privacy complaint report M118-5 as outlined in Appendix A, actions taken and next steps on behalf of the City of Cambridge.
- To ensure compliance with the Municipal Freedom of Information and Privacy Act and the recommendations from the Information and Privacy Commissioner, the City also completed a Privacy Impact Assessment as outlined in Appendix B.

Key Findings

- As a result of a privacy complaint received by the Information Privacy Commissioner (IPC) regarding the installation of a Video Surveillance

System in the Downtown Core as a breach of privacy, an investigation was launched.

- The IPC issued a Privacy Complaint Report, Report No. MI18-5, and provided recommendations to the City to ensure its video surveillance system has been implemented in a manner consistent with the Municipal Freedom of Information and Protection of Privacy Act (*Act*).
- The IPC recommended that the City complete a Privacy Impact Assessment (PIA) to ensure compliance with the *Act*.
- The City is required to report back to the IPC by October 2021 outlining the steps taken as a result of the PIA providing proof of compliance with the recommendations outlined.

Financial Implications

- In 2017 and 2018 Council approved a 3 phased approach for core areas. An operating budget of \$200,000 was assigned for each phase of implementation for the cameras.
- An operating maintenance budget was previously assigned for \$15,000; \$7,500 for 2019 and \$7,500 for 2020, which has been deferred to 2021 due to delays.
- As a result of the IPC investigation a Privacy Impact Assessment was completed within the Clerk's operating budget at a cost of \$13,870.

Background

In 2017, Cambridge Council approved Phase 1 of the Security Camera project report 17-014 (OCM) Single Source Provider for Security Camera Project, Downtown Cambridge (Galt) to enhance a positive and safe environment for the Downtown Cambridge Core area.

In March 2018, as part of Phase 1 of the Camera Project, the City installed ten (10) external video surveillance cameras at 10 different locations consisting of intersections, lots, parking lots and streets in the City's Core Areas.

In May of 2018, Council approved a policy for Camera Surveillance report 18-021 (OCM) Policies - Video Surveillance System attached as Appendix D. This policy is being replaced with an updated policy that reflects risks identified through the PIA and is attached as Appendix E - Use of Corporate Cameras DRAFT Policy. Staff are requesting Council's approval of this updated policy, and will bring updates as required.

The City was notified by the IPC in July 2018, of a privacy complaint related to the camera surveillance specifically related to 10 Cameras in the Galt Core Area and future installation of cameras.

In September 2018, Council approved Phase 2 of the Camera Project report 18-003 (CRE) Single Source Provider for Security Camera Project, Downtown Cambridge (Galt). As part of Phase 2, between September 2019 and December 2019, one camera was installed at the end of the Water Street Pedestrian Bridge and five cameras were installed along the Dan Spring Way Trail.

Phase 3 of the Camera Project Surveillance System Installation for the Preston Towne Centre approved through the 2019 Capital Budget Process.

The privacy complaint was submitted to the Information and Privacy Commissioner (IPC) in July 2018, and since then the investigation has been ongoing.

In December 2020, Council approved Corporate Security Information Report 20-304 (CRS) related to next steps for Security at the City as it relates to staffing. This report advised Council that a new policy would be drafted for the Camera Surveillance System.

The IPC's intent with this investigation was to determine whether the City's video surveillance program is in accordance with the Act and whether it was consistent with the principles and best practices set out in the IPC's guidelines for the use of video surveillance. Further that the City have a PIA completed to ensure compliance.

A Privacy Impact Assessment (PIA) is a risk management process that helps institutions ensure they meet legislative requirements and identify the impacts their programs or activities may have on individuals' privacy.

Privacy risks or impacts fall into two broad categories:

- **Risks to individuals**, including identity theft and other forms of fraud, adverse impact on employment or business opportunities, damage to reputation, embarrassment, distress, or financial impacts.
- **Risks to institutions**, including the financial, legal, and reputational impact of privacy breaches and the consequences of the failure to comply with MFIPPA.

In June of 2021 the City entered into an agreement with PrivacyWorks Inc. for the completion of a Privacy Impact Assessment on the use of Surveillance Cameras within the City of Cambridge. The report from the PIA is attached as Appendix B.

The Phase 1 and Phase 2 of the Galt Core Area implementation of cameras outlined specific locations for the placement of cameras. There are additional cameras throughout the City, including on City facility property and traffic cameras. Due to the nature of the original privacy complaint to the IPC and as part of our due diligence, the City has incorporated all cameras used within the City of Cambridge within the scope of the PIA. Further, all recommendations being implemented as

part of the process will be required to comply with municipal policies as well as legislation. A complete listing of cameras is attached as Appendix C.

Analysis

Strategic Alignment

PEOPLE To actively engage, inform and create opportunities for people to participate in community building – making Cambridge a better place to live, work, play and learn for all.

Goal #2 - Governance and Leadership

Objective 2.4 Work collaboratively with other government agencies and partners to achieve common goals and ensure representation of community interests.

Analysis:

- As a result of the IPC's recommendations a PIA was conducted to ensure that camera surveillance system is necessary to achieve its objectives, to enhance a positive and safe environment and the City's compliance with regards to the collection, use, and retention of personal information under the Municipal Freedom of Information and Protection of Privacy Act. The City has completed a review of existing policies and will be providing further policies to support the operation of its inventory of cameras.

Comments

The City of Cambridge recognizes the need to balance an individual's right to privacy and the need to ensure the safety and security of municipal employees, residents, visitors and property. As an institution governed by the Municipal Freedom of Information and Protection of Privacy Act R.S.O. 1990, Chapter M. 56, the City has obligations with respect to notice, access, use, disclosure, retention, and disposal of records. While video surveillance cameras are installed for safety and security reasons, the Municipality's video surveillance systems must also be designed to minimize privacy intrusion. Proper video surveillance, where deemed necessary, is one of the most effective means of helping to keep Municipal facilities and properties operating in a way that protects security, safety, and privacy. Personal information collected by video surveillance includes video images and audio.

Information and Privacy Commissioner Investigation:

Following the complaint and investigation regarding the City's installation of a video surveillance system in its downtown core areas, the report from the IPC identified the following concerns:

IPC Concern #1 Is the information at issue “personal information” as defined by section 2(1) of the Act? (Personal Information)

City’s Rationale: The City does recognize that the images collected by its video surveillance system is considered to be personal information and therefore subject to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

IPC Findings: The IPC finds that the information at issue qualifies as “personal information” under section 2(1) of the Act.

IPC Concern #2 Is the collection of the personal information in accordance with section 28(2) of the Act? (Collection of Personal Information)

City’s Rationale: The City advised that, pursuant to section 11(1) of the Municipal Act, 2001 the collection of the personal information at issue is necessary to the proper administration of a lawfully authorized activity. The City further advised that there is a real, substantial and pressing problem of public safety to be addressed by the use of its video surveillance system and as evidence of this concern the City advised that there are police reports documenting incidents that have occurred in the Core Areas.

IPC Findings: While the IPC accepts the City’s position and is satisfied that the City’s operation of the Core Areas is a lawfully authorized activity, the IPC must also consider whether the collection of the personal information through the City’s video surveillance system is necessary to the proper administration of its operation of the Core Areas.

The IPC does not conclude that the City’s use of its video surveillance system is not necessary, rather we have not demonstrated that it is necessary, or even necessary to the degree to which it has been implemented.

IPC Concern #3 Is the notice of collection in accordance with section 29(2) of the Act? (Notice of Collection)

City’s Rationales: As required under section 29 of the *Act* the City has placed the signs described in the Surveillance Policy at the public access points to and within areas under surveillance.

IPC Findings: The IPC is satisfied that the City has provided the notice required by section 29(2) and, therefore, finds that Notice of

Collection of the personal information is in accordance with this section.

IPC Concern #4 Is the use of the personal information in accordance with section 31 of the Act? (Consistent Purpose)

City's Rationale: The City advised that the purpose for which it is obtaining or compiling the personal information is "to ensure the safety of the residents and visitors; deter unsafe activities; deter loitering on municipal streets and around public buildings; and contribute to the Cambridge Core Area revitalization. And that, the Surveillance Policy states that, the information collected through video surveillance is used only for the purposes of contributing to the safe environment of the Cambridge Core Area, deterring unsafe activities and assisting as one of the components of Cambridge Core Area revitalization.

IPC Findings: The IPC is satisfied that the personal information collected by the City is used for the same purpose for which it was obtained or compiled.

IPC Concern #5 Is the disclosure of the personal information in accordance with section 32 of the Act? (Where disclosure is permitted)

City's Rationale: While the current policy states that the City does not disclose a video record to any individual or organization except where permitted under the Act, the current practice is to only release footage to a law enforcement agency through a formal request or where requested or subpoenaed by, for search warrants, summons or other order of the courts or a quasi-judicial tribunal. Access to data related to footage shared with law enforcement would require a separate freedom of information request to the law enforcement agency.

IPC Findings: The IPC states that the circumstances in which the City may disclose the personal information are in accordance with sections 32 of the Act.

IPC Concern #6 Is there a right of access to the personal information in accordance with section 36(1) of the Act? (Right of Access to Personal Information)

City's Rationale: The City's Policy under Requests for Disclosure states: The City of Cambridge does not disclose a video record to any individual or organization, except as permitted through MFIPPA. Public requests for disclosure - Any person may

make a written request for access to video records created through a video surveillance system through the freedom of information process. Access may depend on whether there is a justified invasion of another individual's privacy and whether any exempt information can be reasonably severed from the record.

Internal requests for disclosure – City employees or consultants may request a copy of a video recording if it is necessary for the performance of their duties in the discharge of the corporation's function.

Law enforcement requests - The City may disclose a copy of a video recording to a law enforcement agency where there are reasonable grounds to believe that an unlawful activity has occurred and has been captured by the video surveillance system in accordance with section 32. (g) of MFIPPA.

IPC Findings: The IPC finds that there is a right of access to the personal information in accordance with section 36(1) of the *Act*.

IPC Concern #7 **Are there reasonable measures in place to protect the personal information as required by section 3(1) of Ontario Regulation 823 under the *Act*? (Reasonable measures to prevent unauthorized access)**

City's Rationale: In addition to the Surveillance Policy, the City also has a "Code of Conduct" and Privacy Policy which set out relevant procedures concerning the use and disclosure of the personal information collected by the City's video surveillance system and inform City employees that this information must be protected, not inappropriately accessed and handled in accordance with the *Act*.

IPC Findings: The IPC is satisfied that the City has put in place reasonable measures to safeguard the footage collected by its video surveillance system. Therefore, find that there are reasonable measures in place to protect the personal information as required by section 3(1) of O Reg 823 under the *Act*.

IPC Concern #8 **Does the City have proper retention periods in place for the personal information?**

City's Rationale: The City's policy states that in cases where the surveillance system records activities that relate to an insurance, liability, law enforcement, or other similar issue, the appropriate section of

the recording will be copied to suitable media and stored in a separate secure location for a period of no less than one (1) year or a longer appropriate length of time. And that video that has not been requested within the maximum retention period is considered transitory and is automatically erased by being overwritten.

IPC Findings: The IPC is satisfied that the City has provided a reasonable basis after consultation with the video surveillance system provider and the police for retaining the unused video footage for this period. And that the City's retention of the unused personal information collected by the City's video surveillance system is in accordance with the *Act*.

Privacy Impact Assessment

As a result of the IPC Investigation and concerns outlined in their report, the City entered into an agreement to conduct a Privacy Impact Assessment regarding the City's use of cameras. While the initial complaint and investigation from the IPC was related to the Galt Down Town Core area, in the process of gathering information on the city's use of cameras, it was identified that the scope needed to be increased and consequently captured within the scope of the PIA resulting in the following risks:

- PIA Risk #1** It is unknown as to whether the *Policies Governing the Use of Video Surveillance Equipment in City of Cambridge Workplaces* document has been reviewed or updated since 2004.
- PIA Risk #2** It is unknown as to whether the Control Documents for each City Facility are reviewed every two years as stated in the *Policies Governing the Use of Video Surveillance Equipment in City of Cambridge Workplaces* document.
- PIA Risk #3** There is missing information on the systems used and the technical capabilities for a number of the City Facilities.
- PIA Risk #4** The City does not currently have an Individual Access Policy/Procedure or an Employee Acceptable Use Policy which governs the PI under its custody or control.
- PIA Risk #5** There is a risk that the City is not in compliance with section 28(2) of MFIPPA, as there is limited information available on how and why the decision to implement surveillance cameras was made.
- PIA Risk #6** The Alliance Agreement (section 5.2 of this PIA) expired on June 30, 2020. The Alliance Agreement is the camera system service maintenance agreement for phase 1 and 2 cameras.

- PIA Risk #7** It is unknown if the City has entered into other Agreements for the purchasing, use, maintenance, or other considerations related to camera surveillance.
- PIA Risk #8** The City is lacking confidentiality agreements from City employees. There are currently no staff confidentiality agreements or pledge of confidentiality signed by City employees.
- PIA Risk #9** The City's current Privacy Policy does not include the following information:
- Individual's right to make a complaint.
 - Contact information for the Privacy Officer.
 - How to make a complaint to the Privacy Officer Contact information for the IPC.
- PIA Risk #10** There is no standard policy governing the use of the camera movement capabilities. This, coupled with the incomplete information surrounding the technical capabilities of the cameras presents a risk of over-collection of Personal Information.
- PIA Risk #11** City's Privacy Policy is not posted on the website nor is the contact information for the Privacy Officer (City Clerk) easily accessible.

As a result of this risk analysis, a number of recommendations have been developed to mitigate identified privacy risks, close any compliance gaps, and reduce to overall level of residual risk to an acceptable level.

PIA Recommendation #1

Compile information related to how and why the decision to implement surveillance cameras was made.

City Action:

Clerk's staff is currently compiling documentation regarding the implementation of the City's surveillance systems and have reached out to the various community groups involved. (Waterloo Regional Police Service and Cambridge BIA's).

PIA Recommendation #2

It is recommended that the City enact a standard Surveillance Camera Policy, the use of camera surveillance. Policy should include:

- Policy review schedule;
- Access audit schedule;
- Access permissions;
- Acceptable use of recordings;
- How movement capabilities of cameras can be used, in what situation, and by whom.

City Action:

Use of Corporate Camera Policy attached as Appendix D.

PIA Recommendation #3

Compile information regarding any contracts or agreements that the City has entered into in relation to camera surveillance.

City Action:

Clerk's staff is currently compiling an inventory outlining all camera information including location, document status, access permissions, and contact information for each location.

PIA Recommendation #4

The camera system information and technical capabilities of each camera system should be documented in a single document.

City Action:

Clerk's staff currently compiling an inventory all cameras outlining functionality and technical capabilities.

PIA Recommendation #5

It is recommended that the City create and implement the following additional privacy considerations:

- Records Correction Policy and Procedure;
- Complaints Policy and Procedure;
- Privacy training for all City Staff.

City Action:

Staff policies recommended through the PIA are being delivered through training to all staff.

PIA Recommendation #6

Consider implementing an Acceptable Use Policy for all Personal Information (not just camera recordings).

City Action:

Acceptable Use Policy and Procedure for Personal Information being drafted to be implemented by December 2021.

PIA Recommendation #7

Create and implement a Confidentiality Agreement to be signed by staff, in keeping with best practice.

City Action:

Through the implementation of privacy training, Clerk's will be reviewing the recommendation to implement a confidentiality agreement with staff that have access to cameras across the City and will determine how best to ensure of this compliance.

PIA Recommendation #8

Update the City Privacy Policy to include:

- Individual's right to make a complaint;
- Contact information for Privacy Officer;
- How to make a complaint to the Privacy Officer;
- Contact information for the IPC.

City Action:

Clerk's Staff is currently updating the Privacy Policy and reviewing this in connection to the recommendation for confidentiality agreements. This is anticipated to be completed by December 2021.

PIA Recommendation #9

Post the City's Privacy Policy on the public facing website, and include the contact information for the Privacy Officer and the IPC.

City Action:

External City web page being developed to launch by December 2021.

PIA Recommendation #10

Update or renew the Agreement with Alliance.

City Action:

Alliance agreement for Phases 1 and 2 has been extended until such time that Phase 3 cameras are installed. Upon completion of Phase 3 a new maintenance agreement will be entered into outlining coverage for all 3 phases.

PIA Recommendation #11

If feasible, consider consolidating camera systems across the City and creating an electronic access log for recorded footage.

City Action:

The City will pursue consolidation of camera systems upon renewal of systems and will ensure that electronic access control measures are implemented as systems are renewed.

The Clerk is the Municipality's Head under the Municipal Freedom of Information and Protection of Privacy Act ("MFIPPA"), and is responsible for providing a response to access requests.

An internal committee will be developed under the Clerk's supervision to ensure of the following as it relates to camera installation and access:

- Undertaking yearly evaluations of video surveillance system installations to ensure compliance with this Policy.
- Approving installation of video cameras at specified municipally owned and leased properties.
- Advising on placement of video surveillance monitoring signs.
- Acting as the primary contact for all requests from by law enforcement agencies for access to video records.
- Updating and ensuring compliance with all aspects of Security Video Surveillance Policies.
- Ensuring monitoring and recording devices are stored in a safe and secure location.
- Ensuring logbooks, recording all activities related to video devices and records, are kept and maintained.
- Ensuring that no copies of data/images in any format (hardcopy, electronic, etc.) is taken from the video surveillance system inappropriately.
- Immediately taking action with respect to alleged privacy breaches, including investigating video surveillance security privacy breaches and providing quarterly reports to Council.
- Reporting to Council when video surveillance is being proposed in new locations.

Ensuring that staff receive appropriate training. All Staff must adhere to the video surveillance policy and must not access or use information contained in the video surveillance system, its components, files, or database for personal reasons, nor dispose, destroy, erase or alter any record without proper authorization and without following the regulations contained in the Security Video Surveillance Policy.

Existing Policy/By-Law

Provincial Legislation

- The Municipal Freedom of Information and Protection of Privacy Act.

- FIPPA and MFIPPA: Bill 8 — The Recordkeeping Amendments.
- The Municipal Act

City of Cambridge Policies

- City of Cambridge Privacy Policy
- Policy CLK 150-010 Governing the Use of Video Surveillance Equipment in City of Cambridge Workplaces
- Policy CLK 150-020 Governing the Use of Covert Video or Other Types of Surveillance Equipment in City of Cambridge Municipal Work Places
- Surveillance Cameras in the Cambridge Core Areas
- Policy ADM 004 – Surveillance Cameras in the Downtown Core Areas
- Policy HRM 002 – Code of Conduct for Employees

City of Cambridge By-Laws

- By-Law 144-18 To authorized the execution of agreement(s) for the Phase 2 portion of the Video Surveillance System Project with a sole source procurement process pursuant to section 40 of the Purchasing By-Law 133-14

Financial Impact

A one-time cost of \$13,780 was incurred to complete the Privacy Impact Assessment from the City Clerk's Operating Budget.

Public Input

Any member of the public requesting video captured on City Surveillance Cameras is required to submit a request in writing under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

All requests are subject to the provision outlined within the Act.

Signage for all cameras across the City advise the public that the area is under video surveillance.

Internal/External Consultation

External Consultation was completed with the IPC to further understand the report and with PrivacyWorks Consultants Inc for the completion of the PIA.

Conclusion

The City of Cambridge is committed to ensuring and enhancing the safety and security of the public, its employees and property by integrating security best practices with the responsible use of technology. To ensure compliance with legislation and ongoing transparency, staff have worked collaboratively with the IPC to review and implement recommendations as a result of the investigation. The review of the recommendations and the results of the PIA have provided an

opportunity to strengthen current procedures and provide training to staff to build awareness for the use of cameras across the city.

Signature

Division Approval



Name: Danielle Manton

Title: City Clerk

Reviewed by the CFO

Reviewed by Legal Services

Departmental Approval



Name: Dave Bush

Title: Deputy City Manager

City Manager Approval



Name: David Calder

Title: City Manager

Attachments

- Appendix A - IPC Privacy Complaint Report MI18-5
- Appendix B - PrivacyWorks – Privacy Impact Assessment: City of Cambridge Surveillance System
- Appendix C - Camera Inventory
- Appendix D – Surveillance Cameras in the Downtown Core Areas Policy
- Appendix E - Use of Corporate Cameras DRAFT Policy

Information and Privacy Commissioner,
Ontario, Canada



Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT MI18-5

The City of Cambridge

April 23, 2021

Summary: The Office of the Information and Privacy Commissioner of Ontario received a privacy complaint involving the City of Cambridge (the city). The complaint was about the city's installation of a video surveillance system in its downtown core areas. The complainant was concerned that the city's operation of the system breached the privacy of individuals under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*).

This report finds that the city has not conducted an assessment of whether the video surveillance system is necessary to achieve its objectives and recommends that it do so, to ensure compliance with the *Act*.

In the event that the city's assessment determines that the system is necessary and the collection of personal information is thus consistent with the *Act*, this report considers whether the city's notice of collection and use and disclosure of the personal information is in accordance with the *Act*. It also considers whether the city provides a right of access to this information, as well as whether the city has reasonable privacy protection measures and retention periods in place.

This report finds that the city's notice of collection and use and disclosure of the personal information is in accordance with the *Act*. It also finds that there is a right of access to

this information and that the city has reasonable protection measures and proper retention periods in place.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M. 56, as amended, ss. 2(1), 28(2), 29(2), 30(1), 31, 32(a), (d), (g) and (h) and 36(1); *Municipal Act, 2001* S.O. 2001, c. 25, as amended, section 11(1); and *R.R.O. 1990*, Regulation 823, as amended, sections 3(1) and 5.

Orders and Investigation Reports Considered: Privacy Investigation Report MC07-68; Privacy Complaint Reports MC13-46, MC13-60, MC17-32 and PR16-40; and Investigation Report I93-044M.

OVERVIEW:

[1] The Office of the Information and Privacy Commissioner of Ontario (the IPC or this office) received a privacy complaint under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) about the City of Cambridge (the city)'s installation of video surveillance cameras in the Galt Core Area¹.

[2] The complaint alleged that the city's operation of the cameras breached the privacy of individuals under the *Act* and that they had been installed without a policy in place governing their usage.

[3] To address the matter, the IPC opened a Commissioner-initiated privacy complaint file and commenced an investigation to review the city's practices relating to its video surveillance system.

[4] In response, the city, which has a population of over 129,000 people², provided this office with detailed information about its video surveillance system, as well as other relevant information discussed below. The city also provided a copy of its "Surveillance Cameras in the Downtown Core Areas" policy (the Surveillance Policy).³

¹ The Galt Core is one of the city's Core Areas. See <https://www.cambridge.ca/en/learn-about/Downtown-Development-and-Revitalization-Core-Areas.aspx>

² <https://www.investcambridge.ca/en/why-cambridge/demographics.aspx#>

³ This policy, effective September 18, 2019, is the updated version of the city's "Surveillance Cameras in the Cambridge Core Areas" policy that was effective May 15, 2018. The policy is available at: <https://www.cambridge.ca/en/your-city/resources/Policies---Video-Surveillance-System.pdf>

BACKGROUND:***Video Surveillance Camera Installations***

[5] In 2017, to enhance a positive and safe environment for the city's (downtown) Core Areas⁴, the city's council approved Phase 1 of its security camera project (the Camera Project).

[6] In March 2018, as part of Phase 1 of the Camera Project, the city installed ten (10) external video surveillance cameras at 10 different locations consisting of intersections, lots, parking lots and streets in the city's Core Areas.⁵

[7] In May 2018, before any of the video surveillance cameras began recording, the city's council approved the Surveillance Policy pursuant to its Staff Report No: 18-021 OCM (the Staff Report).⁶

[8] The Staff Report's Executive Summary explains that its purpose was to request that the city's Council approve the Surveillance Policy prior to the activation of the Surveillance Cameras. To that end, the Staff Report provides background information about Phase 1 of the Camera Project and discusses how this project strategically aligns with the city's goal of a safe and vibrant downtown Core Area.

[9] Further, the Staff Report contains reasons for the Surveillance Policy, information about other initiatives that have been implemented to achieve the city's goal, as well as, with respect to the project, information about the application of the *Act*, financial impact, public input and internal and external consultation. In conclusion, this report recommended that the city Council approve the Surveillance Policy.

[10] In September 2018, the city's council approved Phase 2 of the Camera Project. As part of Phase 2, between September 2019 and December 2019, one camera was installed at the end of the Water Street Pedestrian Bridge and five cameras were installed along the Dan Spring Way Trail.⁷

[11] According to the city, all of the cameras installed were on the property of the Grand River Conservation Authority⁸ (GRCA) and the city.

[12] The city advised that video recording began in July 2018 and December 2019, respectively, for the cameras installed in Phase 1 and in Phase 2. The city also advised that all of the cameras record 24 hours a day, 7 days a week and that, in accordance

⁴ https://www.cambridge.ca/en/your-city/resources/2018-05-15_18-021OCM-Policies---Video-Surveillance-System.pdf

⁵ The Surveillance Policy defines "Cambridge Core Areas" as the core areas as established by Maps 3, 4 and 5 in the city's Official Plan, namely the Galt City Centre, the Preston Towne Centre, and Hespeler Village, respectively. For detailed information about the camera locations, see section 3.2. of Schedule B to the Surveillance Policy.

⁶ https://www.cambridge.ca/en/your-city/resources/2018-05-15_18-021OCM-Policies---Video-Surveillance-System.pdf

⁷ Section 3.2. of Schedule B to the Surveillance Policy

⁸ The GRCA is a partnership representing watershed municipalities. The city is one of these municipalities. See <https://www.grandriver.ca/en/who-we-are/GRCA-partners.aspx>

with the Surveillance Policy, “signs are posted at public access points to and within areas under surveillance.”

The Surveillance Policy

[13] The Surveillance Policy “applies to municipal video surveillance systems located in the [city’s] Core Areas” and to “all [of the city’s] employees, including full-time, part-time, casual, contract, volunteer and co-op placement employees.”

[14] This policy defines “video surveillance system” as “a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of individuals in public spaces or within City operated facilities.”

[15] It also makes it clear that the city “is responsible for the video surveillance systems and maintaining custody and control of video records at all times on City property.”

DISCUSSION:

[16] The following addresses whether the city’s video surveillance system is in accordance with the privacy protection rules set out in the *Act* relating to the collection, notice, use, disclosure, security and retention of personal information.

[17] In this report, I will refer to the IPC’s *Guidelines for the Use of Video Surveillance* (the Guidelines).⁹ The Guidelines set out best practices for institutions to follow when implementing a video surveillance system.

Issues:

[18] I identified the following issues as arising from this investigation:

1. Is the information at issue “personal information” as defined by section 2(1) of the *Act*?
2. Is the collection of the personal information in accordance with section 28(2) of the *Act*?
3. Is the notice of collection in accordance with section 29(2) of the *Act*?
4. Is the use of the personal information in accordance with section 31 of the *Act*?

⁹ https://www.ipc.on.ca/wp-content/uploads/Resources/2015_Guidelines_Surveillance.pdf

5. Is the disclosure of the personal information in accordance with section 32 of the *Act*?
6. Is there a right of access to the personal information in accordance with section 36(1) of the *Act*?
7. Are there reasonable measures in place to protect the personal information as required by section 3(1) of Ontario Regulation 823 under the *Act*?
8. Does the city have proper retention periods in place for the personal information?

Issue 1: Is the information at issue “personal information” as defined by section 2(1) of the *Act*?

[19] The information at issue is the images of identifiable individuals collected by the city’s video surveillance system.

[20] “Personal information” is defined in section 2(1) of the *Act*, in part, as follows:

“personal information” means recorded information about an identifiable individual, including,

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

[21] Previous decisions by this office have held that information collected about identifiable individuals by video surveillance systems qualifies as “personal information” under the *Act*.¹⁰ The city does not dispute this.

[22] Further, the Surveillance Policy states:

Since images of individuals collected by this video surveillance system are considered to be the personal information of the individuals photographed the recordings are subject to the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).¹¹

[23] Based on the above, I find that the information at issue qualifies as “personal information” under section 2(1) of the *Act*.

¹⁰ Privacy Investigation Report MC07-68 and, Privacy Complaint Reports MC10-2, MC13-46 and MC13-60, all available at: <https://decisions.ipc.on.ca/lpc-cipvp/en/nav.do>

¹¹ Section 1.3 of Schedule B to the Surveillance Policy

Issue 2: Is the collection of the personal information in accordance with section 28(2) of the *Act*?

[24] Section 28(2) of the *Act* requires that the city's video surveillance system collect the personal information only in certain circumstances. This section states:

No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

[25] The city advised that, pursuant to section 11(1) of the *Municipal Act, 2001* (the *Municipal Act*)¹², the collection of the personal information at issue is necessary to the proper administration of a lawfully authorized activity.

[26] Accordingly, first, the city must show that the activity is lawfully authorized and, second, that the collection is necessary to the proper administration of that activity.

[27] Section 11(1) of the *Municipal Act* states:

A lower-tier municipality and an upper-tier municipality may provide any service or thing that the municipality considers necessary or desirable for the public, subject to the rules set out in subsection (4).

[28] The city advised that the lawfully authorized activity is the city's operation of the Core Areas, that is, the city's provision of intersections, lots, parking lots, streets, a bridge and trail within these areas, which under section 11(1) of the *Municipal Act*, the city "considers necessary or desirable for the public".

[29] I accept the city's position in this regard and, therefore, I am satisfied that the city's operation of the Core Areas is a lawfully authorized activity.

[30] Next, I must consider whether the collection of the personal information through the city's video surveillance system is necessary to the proper administration of its operation of the Core Areas.

[31] In *Special Investigation Report* MC07-68, then Commissioner Ann Cavoukian set out what the necessity condition means as follows:

Based on the test established by my office, and adopted by the Court of Appeal, in order to satisfy the necessity condition, the institution must first identify the "lawfully authorized activity" in question, and second, it must

¹² S.O. 2001, c.25

demonstrate how the collection of personal information is “necessary,” not merely helpful, to the achievement of this objective. In addition, this justification must be provided for all classes of personal information that are collected.¹³

[32] Moreover, in the context of video surveillance, the Guidelines discusses the importance of considering the necessity condition with respect to the means used to collect the personal information, as well as the sensitivity and the amount of the personal information collected.¹⁴

[33] Regarding the means used to collect the personal information, the Guidelines advise that it is important that institutions consider whether:

- the problem to be addressed by video surveillance is real, substantial and pressing;
- other less intrusive means of achieving the same goals have been considered and are substantially less effective than video surveillance or are not feasible; and
- the benefits of video surveillance substantially outweigh the reduction of privacy inherent in its use.

[34] The city advised that there is a real, substantial and pressing problem of public safety to be addressed by its video surveillance system. As evidence of this concern, the city advised that there are police reports documenting incidents that have occurred in the Core Areas.

[35] In 2018, as less intrusive means to address public safety concerns, the city advised that it implemented its Ambassador Program.¹⁵ The goals of this program are to enrich the downtown experience in the city, keep the Core Areas clean and well-maintained, and enhance the safe enjoyment and pride in the community.

[36] Members of the Ambassador Program provide safety and security in the Core Areas by having a visible presence, regularly patrolling busy areas, requesting voluntary compliance with the city’s by-laws, checking in with local businesses to address concerns and reporting public disturbances and other issues to the Waterloo Regional Police Service (the police).

[37] Also as less intrusive means, within the Core Areas, the Staff Report advises that the city installed new LED street lights with brighter directed light on certain streets,

¹³ Also, see *Cash Converters Canada Inc. v Oshawa (City)* 2007 ONCA 502 at para.40.

¹⁴ Pages 6 through 10 of the Guidelines

¹⁵ <https://www.cambridge.ca/en/your-city/resources/Booklet-Ambassador-2019-8.5x8.5-WEBSITE-VERSION.pdf>

partnered with the police to ensure bike and foot patrols continue and is working with the three Cambridge business improvement areas to ensure a safe downtown environment.

[38] The city explained that the Ambassador Program and foot patrols have not been as effective as video surveillance because they do not operate 24 hours a day and are limited in size. Further, the city explained that, based on the opinion of the police, these means are less effective than video surveillance.

[39] Regarding the benefits of video surveillance, the city explained that the cameras provide passive surveillance of public areas and permit the police to officially request video recordings through its Clerk's department for specific investigations.

[40] With respect to the sensitivity of personal information, the Guidelines recommend that institutions consider the nature of the space under observation and the "closeness" of the surveillance. The city advised that it considered this and, as a result, all of the cameras are static and have no motorized zoom function.¹⁶

[41] As to the amount of personal information being collected, the Guidelines recommend that institutions apply the principle of data minimization. This principle entails limiting the amount of information collected to that which is necessary to fulfill the purposes of the lawfully authorized activity.

[42] In accordance with the data minimization principle, the city explained that all the cameras are:

- stationary and point at public areas;
- located on property owned by the city or region;
- restricted to prohibit the viewing of locations not intended to be monitored; and
- prevented from looking through window of an adjacent building or areas where a higher level of privacy is expected.

[43] The city also advised that the surveillance system does not have audio capabilities or the ability to collect other sensory information.

[44] At issue is whether the city has demonstrated that the collection of personal information by its video surveillance system is "necessary" and not merely helpful to the

¹⁶ The city advised that the cameras have a limited zoom function, but this must be conducted manually, that is, opening the camera cover and manually zoom the lens while focusing.

proper administration of its operation of the Core Areas. To determine whether the city has shown this, Privacy Complaint Reports MC13-46 and MC13-60 are informative.

[45] In Report MC13-46, Investigator Jeffrey Cutler was not satisfied that a school board's collection of personal information through its video surveillance system was necessary to the proper administration of a lawfully authorized activity. He stated:

I am concerned that there is no additional information to suggest that the guidelines regarding proposals for the installation of video surveillance outlined in Policy I-30 were followed by the Board prior to implementing the video surveillance system in the School. My concern is underscored by the Board's confirmation that it "... did not do a privacy impact assessment or other form of study in relation to the video surveillance program at the [S]chool." Indeed, the decision to employ video surveillance was a part of a broader initiative to implement video surveillance in all secondary schools without apparent detailed consideration to its necessity at this particular facility.

Without the benefit of a privacy impact assessment, security risk assessment or similar analysis, there is no information before me to suggest that the Board considered whether less intrusive means of deterrence, such as increased monitoring by staff, were ineffective or unworkable. Similarly, there is no information indicating that the Board considered the effects of surveillance system would have on personal privacy and whether the design and operation of the video surveillance system minimizes privacy intrusion to that which is necessary, as opposed to simply helpful.

In light of this, the implementation appears pre-emptive, with the only report of a security problem being thefts in the locker room (which are not covered by video surveillance in any case), and a general statement that thefts have not been more or less a problem than in previous years. Aside from this information, there is little material before me to indicate that there were demonstrative security issues at the School prior to the installation of video surveillance cameras.

[46] However, in Report MC13-60, Investigator Cutler was satisfied that a school board's collection of personal information through its video surveillance system was necessary to the proper administration of a lawfully authorized activity.

[47] He came to this conclusion based on a "'School Security Incident Matrix' that classified and listed incidents at the School prior to and after the implementation of video surveillance." Regarding this matrix, Investigator Cutler stated:

The list is comprised of 30 specific incidents over a period of four years, although only once incident occurred after the installation of video cameras. It also identifies loitering and illegal dumping on school property as frequent and ongoing issues. The incidents included intruders in the school building or property, assaults occurring on school property, drug use, theft and vandalism. In many of the instances the Matrix indicates that a police report was filed.

[48] Because of these verifiable and specific reports of incidents, he was satisfied that the matrix demonstrated that the "safety and security events at the School are exceptional in both their severity and frequency".

[49] In this matter, the city explained that its video surveillance system is one of the measures being used to enhance public safety in its operation of the Core Areas. Further, the Staff Report advises that the city's video surveillance system "will be used to ensure the safety of the residents and visitors; deter unsafe activities; deter loitering on municipal streets and around public buildings; and contribute to the Cambridge Core Area revitalization."¹⁷

[50] In my view, using a video surveillance system to help ensure the health, safety and well-being of residents, as well as to protect property, is helpful in achieving the city's safety and security objectives in the Core Areas. Moreover, based on the above, it appears that the city has considered the necessity of the collection of the personal information in accordance with the Guidelines.

[51] As described above, the city relies on police reports, the police's opinion and, the limited size and hours of operation of the Ambassador Program and foot patrols to demonstrate that the collection of personal information by its video surveillance system is necessary, and not merely helpful to the property administration of its operation of the Core Areas.

[52] Further, the city advised that, prior to operating this system, it reviewed the security camera system installed at its City Hall and outlined its video surveillance program with input from a committee composed of community, municipal and law enforcement officials.

[53] However, in determining whether the collection of personal information by a video surveillance system is "necessary", I note the Guidelines explanation of the risks of video surveillance to privacy as follows:

While video surveillance may help to increase the safety of individuals and the security of assets, it also introduces risks to the privacy of individuals whose personal information may be collected, used and disclosed as a result

¹⁷ Section 9.2 of Schedule B to the Surveillance Policy

of the technology. The risk to privacy is particularly acute because video surveillance may, and often does, capture the personal information of law-abiding individuals going about their everyday activities. In view of the broad scope of personal information collected, special care must be taken when considering whether and how to use this technology.

[54] In this matter, the city did not provide me with any verifiable information, statistics or even specific details contained within the (police) reports of incidents that its video surveillance system will address. Moreover, the city advised that it did not conduct a privacy impact assessment, or similar analysis, before or after installing this system.

[55] Although the city advised that there is a public safety problem that is being addressed by its video surveillance system, I have nothing before me beyond its broad assertion that this problem is real, substantial or pressing, or that the less intrusive means in place are substantially less effective than this system. As a result, I find that the city has not shown that the benefits of its video surveillance system outweighs the reduction of privacy inherent in its use.

[56] For these reasons, I am not satisfied that the city has demonstrated that the collection of personal information by its video surveillance system is "necessary" and not merely helpful to the proper administration of its operation of the Core Areas.

[57] Accordingly, I am not satisfied that this collection is necessary to the proper administration of a lawfully authorized activity. Therefore, I find that the collection of the personal information by the city's video surveillance system is not in accordance with section 28(2) of the *Act*.

[58] By this finding, I am not concluding that the city's use of its video surveillance system is not necessary, per se. Rather, I conclude that the city has not demonstrated that it is necessary, or even necessary to the degree to which it has been implemented.

[59] To address this conclusion, I will recommend that the city conduct an assessment (such as, a privacy impact assessment) of its video surveillance system in accordance with the *Act*, the Surveillance Policy and this report. Doing so will help the city determine the potential, actual and type of effects that its video surveillance system may have on personal privacy. It will also help in determining the steps the city should take to mitigate those effects and minimize privacy intrusion to that which is necessary to achieve its lawful goals.

[60] Following an assessment of its video surveillance system, should the city determine that it is necessary, I recommend that the city implement the system in the Core Areas in accordance with the *Act*, the Surveillance Policy and this report.

[61] Findings regarding the city's notice of collection, use, disclosure, protection and retention of the personal information are contingent upon the valid collection of this information by its video surveillance system and, given my determination above, may not be strictly necessary at this time.

[62] However, these additional issues are before me and my findings on them will be applicable if, following an assessment(s), the city determines that its video surveillance system is necessary and implemented in a manner consistent with the *Act*, the Surveillance Policy and this report. Moreover, the results of this investigation and an analysis of the city's efforts to comply with the *Act* will be instructive to the city, stakeholders and other institutions.

[63] Therefore, as the city's video surveillance system is collecting personal information and the city may determine that it is necessary to the proper administration of a lawfully authorized activity in accordance with section 28(2) of the *Act*, I will consider whether the city's notice of collection, use, disclosure, protection and retention of the personal information is in accordance with the *Act*.

Issue 3: Is the notice of collection in accordance with section 29(2) of the *Act*?

[64] Because the city's video surveillance system collects the personal information from individuals, generally, section 29(2) of the *Act* requires that they receive notice of the collection. This section states:

If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,

- (a) the legal authority for the collection;
- (b) the principal purpose or purposes for which the personal information is intended to be used; and
- (c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection.

[65] To give individuals notice, the Guidelines suggest that institutions make the notice required by section 29(2) available and easily accessible on their website. The Guidelines also recommend that, at the perimeter of the monitored areas and at key locations within these areas, institutions place signs with a clear, language-neutral graphical depiction of

the use of a video surveillance that also contain basic information clarifying that video surveillance is being used.¹⁸

[66] In this matter, the Surveillance Policy containing the notice required by section 29(2) is available and accessible online.¹⁹ Further, it provides that “written notice, in easily readable lettering, will be posted in the public area in a position easily viewed by the public” and that signs will have a clear, language neutral graphical depiction of the use of video surveillance and state:

To promote safety this area is under video surveillance.

Images may be recorded and/or monitored.

Information collected by the use of video equipment in this area is collected under the authority of the Municipal Act, 2001 in accordance with the provisions of the Municipal Freedom of Information and Protection of Privacy Act.

Any questions about this collection can be obtained by contacting City Clerk’s Office at 519-740-4680 ext 4583.²⁰

[67] As previously mentioned, the city advised that it has placed the signs described in the Surveillance Policy at the public access points to and within areas under surveillance.

[68] Based on the above, I am satisfied that the city has provided the notice required by section 29(2) and, therefore, I find that the notice of collection of the personal information is in accordance with this section.

Issue 4: Is the use of the personal information in accordance with section 31 of the *Act*?

[69] Section 31 of the *Act*, generally, prohibits the city’s use of the personal information collected by its video surveillance system unless one of the exceptions under this section applies.

[70] Section 31 states:

An institution shall not use personal information in its custody or under its control except,

¹⁸ This recommendation assumes that a high percentage of the individuals whose personal information is being collected are able to read the signs (that is, are not visually disabled).

¹⁹ <https://www.cambridge.ca/en/your-city/resources/Policies---Video-Surveillance-System.pdf>

²⁰ Sections 2.1 and 10.1 of Schedule B to the Surveillance Policy

- (a) if the person to whom the information relates has identified that information in particular and consented to its use;
- (b) for the purpose for which it was obtained or compiled or for a consistent purpose; or
- (c) for a purpose for which the information may be disclosed to the institution under section 32 or under section 42 of the *Freedom of Information and Protection of Privacy Act*.

[71] Further, with respect to the use of personal information in the context of video surveillance, the Guidelines provide the following explanation:

In the context of video surveillance, this means that as a general rule, institutions may only use personal information collected by means of video surveillance for the purpose of the video surveillance program or for a consistent purpose. Use of the information for other, unrelated purposes would not generally be permitted. When information collected for one purpose is used for another, unrelated purpose this is often called 'function creep.'

[72] In this matter, in my view, section 31(b) of the *Act* sets out the most applicable exception that would allow the city to use the personal information. To see whether this section applies, first, the purpose for which the personal information was obtained or compiled must be determined, and, second, whether the use of this information has taken place for either the same purpose or a consistent purpose must be determined.

[73] As previously mentioned, the city advised that the purpose for which it is obtaining or compiling the personal information is "to ensure the safety of the residents and visitors; deter unsafe activities; deter loitering on municipal streets and around public buildings; and contribute to the Cambridge Core Area revitalization."

[74] Regarding the use of the collected information, the Surveillance Policy states:

Use of video recordings – the information collected through video surveillance is used only for the purposes of contributing to the safe environment of the Cambridge Core Area, deterring unsafe activities and assisting as one of the components of Cambridge Core Area revitalization.

[75] Based on the above, I am satisfied that the personal information collected by the city is used for the same purpose for which it was obtained or compiled.

[76] Accordingly, I find that the city's use of the personal information is in accordance with section 31(b) of the *Act* and, therefore, I find that the use of the personal information is in accordance with section 31 of the *Act*.

Issue 5: Is the disclosure of the personal information in accordance with section 32 of the *Act*?

[77] According to the Surveillance Policy, the city discloses the personal information collected by its video surveillance system as follows:

The City of Cambridge does not disclose a video record to any individual or organization except as permitted through MFIPPA.

1. Public requests for disclosure – Any person may make a written request for access to video records created through a video surveillance system through the freedom of information process. Access may depend on whether there is a justified invasion of another individual's privacy and whether any exempt information can be reasonably severed from the record. (through appropriate request form)

2. Internal requests for disclosure – City employees or consultants may request a copy of a video recording if it is necessary for the performance of their duties in the discharge of the corporation's function.

3. Law enforcement requests – The City may disclose a copy of a video recording to a law enforcement agency where there are reasonable grounds to believe that an unlawful activity has occurred and has been captured by the video surveillance system in accordance with section 32(g) of MFIPPA (through appropriate request form).

[78] The Surveillance Policy also states:

The Freedom of Information Co-ordinator (or designate) is permitted to release copies of the records to a law enforcement agency in response to a verbal request only in situations involving an emergency, imminent danger or hot pursuit. All other requests for access by law enforcement authorities must be documented through the access request documentation utilized routinely by the Freedom of Information Co-ordinator.²¹

²¹ Section 6.4 of Schedule B to the Surveillance Policy

[79] Further, the Surveillance Policy provides that “recordings must be released if they are subject to a subpoena, search warrant, summons or other order of the courts or a quasi-judicial tribunal.”²²

[80] Section 32 of the *Act* prohibits the disclosure of the personal information by the city unless one of the exceptions described in paragraphs (a) to (l) under this section applies.

[81] Section 32, in part, states:

An institution shall not disclose personal information in its custody or under its control except,

(a) in accordance with Part I;

...

(d) if the disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and if the disclosure is necessary and proper in the discharge of the institution's functions.

...

(g) if disclosure is to an institution or a law enforcement²³ agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;

(h) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification is mailed to the last known address of the individual to whom the information relates;

Section 32(a)

[82] The Surveillance Policy provides that the city may disclose the personal information in response to a written access request made through the freedom of information process. In my view, the exception set out in section 32(a) of the *Act* would apply to this type of disclosure.

²² Section 7.2 of Schedule B of the Surveillance Policy

²³ “Law enforcement” is defined in section 2(1) of the *Act* as (a) policing, (b) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or (c) the conduct of proceedings referred to in clause (b).

[83] Section 32(a) allows the disclosure of personal information in accordance with Part I of the *Act*, which governs freedom of information and access to records in the custody or control of institutions.

[84] Therefore, disclosure of the personal information in response to an access request that is done in accordance with Part I would be a permitted disclosure under section 32(a).

[85] Accordingly, I find that the city's disclosure of the personal information in response to written public access requests made under the freedom of information process, that is, the *Act*, would be in accordance with section 32(a).

Section 32(d)

[86] The Surveillance Policy provides that the city may disclose the personal information in response to internal requests. In my view, the exception set out in section 32(d) of the *Act* would apply to this type of disclosure.

[87] Previous decisions by this office have identified the following three conditions that must be met for section 32(d) to apply:

1. The disclosure must be made to an officer, employee, consultant or agent;
2. Who needs the information in the performance of their duties; and
3. The disclosure must be necessary and proper in the performance of the institution's functions which includes the administration of statutory programs and activities necessary to the overall operation of the institution.²⁴

[88] Section 32(d) makes it clear that a disclosure of personal information even within an institution must be justified and will be subject to scrutiny on a "need to know basis." The sharing of information pursuant to this section must be based on more than "mere interest or concern".²⁵

[89] As indicated above, the Surveillance Policy provides that the personal information may be disclosed to an employee or consultant "if it is necessary for the performance of their duties in the discharge of the [city's] function."

²⁴ Privacy Complaint Reports MC11-73 and MC-050034-1, Investigation Reports I95-007M and I96-113P and Order PO-1998

²⁵ See *H. (J.) v. Hastings (County)* (1993), 12 M.P.L.R. (2d) 40 (Ont. Ct. Gen. Div.)

[90] For this reason, I am satisfied that the conditions required for section 32(d) to apply have been met.

[91] Therefore, I find that the city's disclosure of the personal information in response to an internal request would be in accordance with section 32(d).

Section 32(g)

[92] The Surveillance Policy provides that the city may disclose the personal information in response to requests from law enforcement agencies in accordance with section 32(g) of the *Act*.

[93] Specifically, this policy advises that such disclosure would occur "where there are reasonable grounds to believe that an unlawful activity has occurred and has been captured by the video surveillance system" or where the information is "subject to subpoena, search warrant, summon or other order of the courts or a quasi-judicial tribunal."

[94] Based on these conditions under which the city would disclose the personal information to a law enforcement agency, in my view, such disclosure would be an aid "to an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result."

[95] Therefore, I find that the city's disclosure of the personal information in response to a request from a law enforcement agency would be in accordance with section 32(g).

Section 32(h)

[96] The Surveillance Policy provides that the city may disclose the personal information to a law enforcement agency "in response to a verbal request only in situations involving an emergency, imminent danger or hot pursuit." In my view, the exception set out in section 32(h) of the *Act* would apply to this type of disclosure.

[97] Based on the purposes for which the city uses the personal information, that is, safety and security, in my view, it is reasonably foreseeable that "in situations involving an emergency, imminent danger or hot pursuit", these uses might require the disclosure of the personal information in such "compelling circumstances affecting the health or safety of an individual."

[98] Therefore, I find that the city's disclosure of the personal information in response to a verbal request from a law enforcement agency in the specified situations would be in accordance with section 32(h).

[99] As I have found that the circumstances in which the city may disclose the personal information are in accordance with sections 32(a), (d), (g) or (h), I find, therefore, that the disclosure of the personal information is in accordance with section 32 of the *Act*.

Issue 6: Is there a right of access to the personal information in accordance with section 36(1) of the *Act*?

[100] Section 36(1) of the *Act* gives individuals a right of access to their personal information collected by the city's video surveillance system. This section states:

Every individual has a right of access to,

- (a) any personal information about the individual contained in a personal information bank in the custody or under the control of an institution; and
- (b) any other personal information about the individual in the custody or under the control of an institution with respect to which the individual is able to provide sufficiently specific information to render it reasonably retrievable by the institution.

[101] Moreover, to protect personal information when responding to access requests, the Guidelines advise that an institution's "video surveillance system should include the ability to remove or redact information from the video footage to protect exempted information."

[102] As indicated above, the Surveillance Policy provides that individuals "may make a written request for access to video records created through a video surveillance system through the freedom of information process."

[103] Further, the city advised that its video surveillance system can black out or blur images and confirmed that, pursuant to section 36(1), individuals can access their personal information collected by it.

[104] For these reasons, I find that there is a right of access to the personal information in accordance with section 36(1) of the *Act*.

Issue 7: Are there reasonable measures in place to protect the personal information as required by section 3(1) of Ontario Regulation 823 under the *Act*?

[105] Section 3(1) of Ontario Regulation 823 (O Reg 823) requires that the city “ensure that reasonable measures to prevent unauthorized access to [individuals’ information] are defined, documented and put in place, taking into account the nature of the records to be protected.” This requirement “applies throughout the life-cycle of a given record, from the point at which it is collected or otherwise obtained, through all of its uses, and up to and including its eventual disposal.”²⁶

[106] In Investigation Report I93-044M, then Assistant Commissioner Ann Cavoukian stated the following about the term “reasonable measures” in section 3(1) of O Reg 823:

The determination of whether reasonable measures had been put into place hinges on the meaning of “reasonable” in section 3(1) of Regulation 823, R.R.O. 1990, as amended. Black’s Law Dictionary defines reasonable as:

Fair, proper, just, moderate, suitable under the circumstances. Fit and appropriate to the end in view ... Not immoderate or excessive, being synonymous with rational, honest, equitable, fair, suitable, moderate, tolerable.

Thus, for reasonable measures to have been put into place would not have required a standard so high as to necessitate that every possible measure be pursued to prevent unauthorized access. In our view, the measures identified above are consistent with Black’s definition of “reasonable” -- appearing to be fair and suitable under the circumstances.

[107] Moreover, in Privacy Complaint Report PR16-40, then Investigator Lucy Costa stated the following about section 4(1) of Regulation 460 (which is the provincial access/privacy law equivalent of section 3(1) of O Reg 823):

From the way this section of the regulation is written, it is clear that it does not prescribe a “one-size-fits-all” approach to security. It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have “reasonable” measures and ties those measures to the “nature” of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions.

²⁶ Privacy Complaint Report MI10-5

[108] Regarding video surveillance, generally, security measures should include:

- administrative measures, such as the development of clear policies and procedures regarding use and disclosure;
- technical measures, such as ensuring that images are encrypted and that robust controls are in place that ensure only those who need the information can access it (this includes logging and auditing); and
- physical measures, such as ensuring secure locations for video monitors and image storage.²⁷

[109] Further, the Guidelines advise that, “in the context of video surveillance, security involves ensuring the confidentiality, integrity and availability of the footage captured by the system.” To that end, the Guidelines set out measures that institutions may take.²⁸

[110] The city provided this office with relevant information regarding the security measures in place for its video surveillance system. Some of these details are not set out in this report because disclosing them might compromise the effectiveness of these measures.

[111] Regarding administrative measures, in addition to the Surveillance Policy, the city also has a “Code of Conduct For the Employees of the City Of Cambridge” and a “City of Cambridge Privacy Policy”.²⁹ These documents set out relevant procedures concerning the use and disclosure of the personal information collected by the city’s video surveillance system and inform city employees that this information must be protected, not inappropriately accessed and handled in accordance with the *Act*.

[112] Further, the city advised that it holds privacy workshops and training for staff who access its video surveillance system and that they are required to sign a confidentiality agreement.

[113] Regarding technical measures, the city advised that video footage is encrypted and access to it is password protected. The city also advised that it would provide individuals who are able to view the footage with an auditable unique login to its video surveillance system.

[114] In addition, the Surveillance Policy specifies that the monitor can only be viewed by the city’s Director of Economic Development (or designate), Manager of Technology and Support Services, and Corporate Property Manager.³⁰ This policy also specifies that

²⁷ Page 3 of the IPC Fact Sheet: Video Surveillance available at: <https://www.ipc.on.ca/wp-content/uploads/2016/11/2016-00-09-video-surveillance.pdf>

²⁸ Page 17 of the Guidelines

²⁹ <https://www.cambridge.ca/en/your-city/resources/Code-of-Conduct-for-the-Employees.pdf> and <https://www.cambridge.ca/en/your-city/resources/Privacy-Policy---June-2014.pdf>

³⁰ Section 4.1 of Schedule B of the Surveillance Policy

only these individuals and the city's Freedom of Information Co-ordinator (or their designate) can view recorded footage, which "must be conducted in private and in the presence of authorized persons only", or access it."³¹ Moreover, if required, access to recorded footage by the city's Technology Services staff "is limited to ensuring the system functions according to specifications."³²

[115] With respect to live viewing of footage, the Surveillance Policy states:

Live viewing is restricted to time periods when there is higher likelihood of safety and security concerns, or the commission of unauthorized activity in the area under surveillance. Live feed monitors are turned off when not in use.

[116] When disclosing personal information in accordance with the *Act*, the Guidelines advise that "it is important that disclosures be done in a manner that protects the privacy and security of the personal information." To that end, the Guidelines recommend that institutions maintain an auditable log of each disclosure and ensure that this log contains certain information.

[117] The Surveillance Policy requires that "requests for access [to video footage] by law enforcement authorities must be documented through the access request documentation utilized routinely by the FOI co-ordinator."³³ In addition, it provides that access to video footage will be logged as follows:

A log will be kept to record access to the recordings. An entry will be made each time the recordings are consulted or any time a copy is made of any part of them. The log entry will note the person(s) accessing the recordings and the reason for access.³⁴

[118] Based on my review of the logs used by the city when it discloses the personal information collected by its video surveillance system, generally, I am satisfied that these forms contain the information recommended by the Guidelines.³⁵

[119] With respect to system review and audits, the Guidelines recommend that institutions regularly audit the roles, responsibilities and practices of its video surveillance program regularly to ensure that they comply with its policies and procedures.

[120] To this end, the city advised that it audits the logs annually and that its staff can perform random audits. Further, the city advised that its policies must be reviewed in

³¹ Sections 6.3 and 6.5 of Schedule B to the Surveillance Policy

³² Sections 5.2, 6.3 and 6.5 of Schedule B to the Surveillance Policy

³³ Section 6.4 of Schedule B to the Surveillance Policy

³⁴ Section 7.1 of Schedule B to the Surveillance Policy

³⁵ Pages 14 to 15 in the Guidelines

2024 and that its video surveillance system is checked once a year to ensure that all of the cameras are pointed correctly and are operating sufficiently.

[121] Regarding physical measures, according to the Surveillance Policy, “the recording and storage equipment will be stored in a secure, non-public area at all times” and that “one secure monitor is located in the Office of the Corporate Property Manager.”³⁶ The city also advised that it would restrict devices capable of recording (for example, cell phones) from this manager’s office.

[122] Based on the above, I am satisfied that the city has put in place reasonable measures to safeguard the footage collected by its video surveillance system. Therefore, I find that there are reasonable measures in place to protect the personal information as required by section 3(1) of O Reg 823 under the *Act*.

Issue 8: Does the city have proper retention periods in place for the personal information?

[123] Section 30(1) of the *Act* requires that the city keep the personal information collected by its video surveillance system “for the period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the personal information.”

[124] To that end, section 5 of O Reg 823 prescribes the following period:

An institution that uses personal information shall retain it for the shorter of one year after use or the period set out in a by-law or resolution made by the institution or made by another institution affecting the institution, except if,

- (a) the individual to whom the information relates consents to its earlier disposal; or
- (b) the information is credit or debit card payment data.

[125] Together, section 30(1) and section 5 of O Reg 823 establish a default minimum one-year retention period for used personal information,³⁷ subject to the exceptions set out in section 5 of O Reg 823.

³⁶ Sections 4.1 and 6.1 of Schedule B to the Surveillance Policy

³⁷ Privacy Complaint Reports MC10-2, MC13-46, MC13-60 and MC17-32

Used Video Footage

[126] Where video footage has been used, it would be subject to the one-year minimum retention period indicated above. The Guidelines advise that, “in the context of video surveillance, personal information is used whenever footage that contains images of individuals or other identifiable information is accessed or disclosed.” It also advises that, “simply viewing a live feed does not represent a ‘use’ of personal information”.

[127] Regarding used video footage, the Surveillance Policy states:

In cases where the surveillance system records activities that relate to an insurance, liability, law enforcement or other similar issue, the appropriate section of the recording will be copied to suitable media and stored in a separate secure location for a period of no less than one (1) year or a longer appropriate length of time.³⁸

[128] For this reason, I am satisfied the city’s retention period for used personal information is in accordance with the minimum one-year retention period.

[129] Therefore, I find that the retention of used personal information is in accordance with section 30(1) of the *Act*.

Unused Video Footage

[130] Where video footage has not been used, the Guidelines recommend that its retention period be limited as follows:

Recorded information that has not been used is routinely erased according to a standard schedule. Under the standard schedule, the retention period for unused information is limited to the amount of time reasonably necessary to discover or report an incident that occurred in the space under surveillance.³⁹

[131] The Guidelines also advise that “when erasing or deleting recorded information, whether used or unused, it is critical that the information and old storage devices are disposed of in such a way that the personal information cannot be reconstructed or retrieved.”⁴⁰

[132] The city advised that unused video footage is retained until its system’s electronic storage capacity is reached or up to 30 days, whichever comes first. Once capacity is reached or 30 days have passed, the city explained that the unused footage is

³⁸ Section 6.2 of Schedule B to the Surveillance Policy

³⁹ Page 10 of the Guidelines

⁴⁰ Page 11 of the Guidelines

permanently erased, that is, overwritten. The city further explained that it chose a (maximum) 30-day schedule based on the opinions of both the provider of its video surveillance system and the police.

[133] I am satisfied that the city has provided a reasonable basis after consultation with the video surveillance system provider and the police for retaining the unused video footage for this period.

[134] For this reason, I am satisfied that the retention of the unused personal information collected by the city's video surveillance system is in accordance with the *Act*.

[135] Therefore, I find that the city has proper retention periods in place for the personal information.

The city's consultation with stakeholders

[136] The *Act* does not require that institutions consult with anyone about the collection of personal information where such collection is necessary to the proper administration of a lawfully authorized activity.

[137] However, the Guidelines recommends that individuals who might be affected by video surveillance should be consulted as follows:

The use of video surveillance affects all the individuals who end up moving within the space under observation. Therefore, prior to using video surveillance, and where feasible to do so, [an institution] should identify those who reasonably may be affected by the video surveillance and consult with them as to the program's necessity and impact.⁴¹

[138] The matter of consultation raises two questions. The first question is: who are the stakeholders? For this question, "context is important, and in each circumstance where the installation of cameras is considered the questions should be asked who may be reasonably affected by the video surveillance? And, is consultation feasible?"⁴²

[139] The second question is: were the stakeholders adequately consulted?⁴³ Consultation is more than merely announcing the decision to implement video surveillance.⁴⁴

⁴¹ Page 19 of the Guidelines

⁴² Privacy Complaint Report MC13-60.

⁴³ Privacy Complaint Report MC13-60.

⁴⁴ Privacy Complaint Reports MC13-60 and MC13-67.

[140] The city advised that camera placement was determined with input from the police and the Downtown Cambridge Business Improvement Area based on their experience with the city's downtown activities, as well as from the Regional Municipality of Waterloo.

[141] The city also advised that a committee of community, municipal and law enforcement stakeholders came together to outline the video surveillance program. Further, the Staff Report lists various internal and external stakeholders that the city consulted regarding its video surveillance program.

[142] Moreover, as previously indicated, the city's council approved the Surveillance Policy before any of the video surveillance cameras began recording.

[143] In light of the aforementioned steps taken, I commend the city for its consultations with stakeholders regarding the implementation of its video surveillance system.

CONCLUSION:

Based on the results of my investigation, I have reached the following conclusions:

1. The information at issue is "personal information" as defined by section 2(1) of the *Act*.
2. The collection of the personal information is not in accordance with section 28(2) of the *Act*.
3. The notice of collection is in accordance with section 29(2) of the *Act*.
4. The use of the personal information is in accordance with section 31 of the *Act*.
5. The disclosure of the personal information is in accordance with section 32 of the *Act*.
6. There is a right of access to the personal information in accordance with section 36(1) of the *Act*.
7. There are reasonable measures in place to protect the personal information as required by section 3(1) of Ontario Regulation 823 under the *Act*.
8. The city has proper retention periods in place for the personal information.


9. The city properly consulted with stakeholders.

RECOMMENDATIONS:

Based on the above conclusions, I make the following recommendations:

1. I recommend that the city conduct an assessment of its video surveillance system in a manner consistent with the *Act*, the Surveillance Policy and this report, to determine whether the collection of personal information by the system is necessary to the proper administration of a lawfully authorized activity in accordance with section 28(2) of the *Act*.
2. Following an assessment of the video surveillance system and assuming a determination by the city that it is necessary, I recommend that the city implement the system in a manner consistent with the *Act*, the Surveillance Policy and this report.
3. Within six months of receiving this report, the city should provide this office with proof of compliance with the above recommendations.

The city has reviewed this report and agreed to implement the above recommendations. Accordingly, within six months of receiving this report, the city should provide this office with proof of compliance with these recommendations.



John Gayle
Investigator

April 23, 2021

Privacy Impact Assessment

City of Cambridge Surveillance System

Table of Contents

Table of Contents.....	2
1. Introduction	3
1.1. Executive Summary.....	3
1.2. Background	3
1.3. PIA Scope.....	5
2. Business Process	5
2.1. Target Description Overview (Program/System Overview).....	5
2.2. Stakeholders	7
3. System Description	8
3.1. Camera Locations.....	8
4. Information Management	13
4.1. System Access Controls.....	13
4.2. Logging and Auditing.....	14
5. Privacy Analysis.....	15
5.1. Provincial Statutes	15
5.2. Contracts and Agreements	17
5.3. Dataflow and Legislative Authority.....	19
6. Privacy Principles	20
6.1. Principle 1 – Accountability.....	20
6.2. Principle 2 – Identifying Purposes.....	21
6.3. Principle 3 – Consent	22
6.4. Principle 4 – Limiting Collection.....	24
6.5. Principle 5 – Limiting use, Disclosure, and Retention.....	24
6.6. Principle 6 – Accuracy	26
6.7. Principle 7 – Safeguards.....	26
6.8. Principle 8 – Openness.....	27
6.9. Principle 9 – Individual Access	28
6.10. Principle 10 – Challenging Compliance	29
7. Risk Assessment.....	31
8. Recommendations	33
Appendix A – Risk Rating Methodology.....	35
Appendix B – Publicly Available Police Generated Statistics	36
Appendix C – Individual Access Request Form	37
Appendix C – Individual Access Request Form Continued.....	38
Appendix D – Police Access Request Form	39
Appendix E – Cambridge Privacy Policy	40

1. Introduction

1.1. Executive Summary

This Privacy Impact Assessment (“PIA”) is being conducted on behalf of the City of Cambridge, on the current surveillance camera program within the municipality.

In the course of the assessment, 11 risks were noted. The risks, as described throughout the PIA and in detail in section 7, are as follows:

Risk #	Description
1	It is unknown as to whether the <i>Policies Governing the Use Of Video Surveillance Equipment in City Of Cambridge Workplaces</i> document has been reviewed or updated since 2004.
2	It is unknown as to whether the Control Documents for each City Facility are reviewed every two years as stated in the <i>Policies Governing the Use Of Video Surveillance Equipment in City Of Cambridge Workplaces</i> document.
3	There is missing information on the systems used and the technical capabilities for a number of the City Facilities.
4	The City does not currently have an Individual Access Policy/Procedure or an Employee Acceptable Use Policy which governs the PI under its custody or control.
5	There is a risk that the City is offside section 28(2) of MFIPPA, as there is limited information available on how and why the decision to implement surveillance cameras was made.
6	The Alliance Agreement (section 5.2 of this PIA) expired on June 30, 2020.
7	It is unknown if the City has entered into other Agreements for the purchasing, use, maintenance or other considerations related to camera surveillance.
8	There are currently no staff confidentiality agreements or pledge of confidentiality signed by City employees.
9	The City’s current Privacy Policy does not include the following information: <ul style="list-style-type: none"> • Individual’s right to make a complaint • Contact information for the Privacy Officer • How to make a complaint to the Privacy Officer • Contact information for the IPC
10	There is no standard policy governing the use of the camera movement capabilities. This, coupled with the incomplete information surrounding the technical capabilities of the cameras presents a risk of over-collection of PI.
11	City’s Privacy Policy is not posted on the website nor is the contact information for the Privacy Officer (City Clerk) easily accessible.

1.2. Background

In 2017, Cambridge City Council approved Phase 1 of the Security Camera project to “enhance a positive and safe environment for the Downtown Cambridge Core Area”¹. The project was completed in 2018.

¹ Policies – Video Surveillance System Document, Report 18-021 OCM.

In addition to the cameras installed in the Downtown Core Area (“Downtown Core Area cameras”), there are multiple stand-alone surveillance systems throughout Cambridge, located in City-run facilities, buildings, and areas (“City Facilities Cameras”). A list and descriptions of these camera surveillance systems can be found in section 3.1 of this document.

Downtown Core Area Cameras

The Downtown Core Area cameras were installed and operationalized by 2018, and are governed under the City’s *Surveillance Cameras in the Downtown Core Areas* Policy. As determined by Cambridge City Council in conjunction with the local police force (Waterloo Regional Police) and public consultations, surveillance cameras were installed in the Downtown Core Area where there was a higher perceived risk of crime. The stated objectives of these surveillance systems are to ensure the safety of residents and visitors, deter unsafe activities, and deter loitering on municipal streets and around public buildings.

Prior and in conjunction to the installation of these cameras, the City created the Ambassador program as a less intrusive strategy against public safety concerns. The Ambassador program is staffed by volunteers from the community who “walk through the three core areas of Galt, Preston and Hespeler to provide maintenance, ambassador and beautification services.”² Ambassador services include “requesting voluntary compliance with City ordinances”³.

Additionally, the City installed LED street lights with directed lights on certain streets and have partnered with police to ensure there are bike and foot patrols throughout the Downtown Core Area.

The City reported limited success with these less intrusive strategies, and were advised by police that they were not as effective as camera surveillance.

City Facilities Cameras

The history and initiation dates for the City Facilities Cameras are unknown as each system is managed by the specific facility, leading to a gap in record keeping and institutional knowledge. This will be discussed in further detail in section 5.1.

There is a *Policies Governing the Use Of Video Surveillance Equipment in City Of Cambridge Workplaces* (“Video Surveillance Policy”) document, drafted in 2004, which provides some guidelines on the governance of surveillance camera systems within City Facilities. It is relevant to note that this Policy has not been updated since 2004, and it is unknown as to whether it has been reviewed since its creation or is still in effect. This has been logged as risk 1 in section 7.

For both the City Facilities and the Downtown Core Area Cameras, the City of Cambridge is responsible for the camera surveillance systems and maintains custody and control of video recordings. The collection of personal information through video surveillance is governed under the *Municipal Freedom of Information and Protection of Privacy Act* (“MFIPPA”).

² [Ambassador Program - City of Cambridge](#)

³ [Ambassador Program - City of Cambridge](#)

1.3. PIA Scope

This PIA covers the City's use of camera surveillance on its citizens, and the collection, use, disclose, and access to camera recordings and live streams for the Downtown Core Area and City Facilities.

Out of Scope:

A review of the technical security aspects for the camera systems are out of scope for this PIA as is the Ambassador program.

2. Business Process

2.1. Target Description Overview (Program/System Overview)

As described above in section 1.2, there are a number of distinct camera systems within the City of Cambridge.

Downtown Core Area Cameras

The Downtown Core Area cameras are governed under the City's *Surveillance Cameras in the Downtown Core Areas Policy*.

The Downtown Core Area cameras are owned and operated by the city, and are comprised of two distinct systems, the recordings for which are both stored on the city servers located in City Hall. Per the *Surveillance Cameras in the Downtown Core Areas Policy* recordings are kept for 30 days if no access request has been made for the recordings. In cases where an access request has been made by either an individual or police, the recordings will be retained for a year or longer as appropriate.

City Facilities Cameras

Each of the camera systems operating at a City Facility is managed by that specific facility and the associated Control Document. These Control Documents are unique to each facility, however, they use a common template.

Regarding the Control Documents, the Video Surveillance Policy states:

"Whenever the installation of video surveillance equipment is being considered within the City of Cambridge's offices or in any other municipal workplace the head of the department considering the installation or staff members to whom the department head has delegated authority will prepare, in conjunction with the city's Freedom of Information co-ordinator, a comprehensive written control document for the operation of that particular system. At a minimum this control document will contain all the information outlined in the procedures prepared in conjunction with this policy."⁴

The Video Surveillance Policy goes on to state that the control document for each surveillance camera installation shall be reviewed and updated at least every two years by an audit team that will include the city's Freedom of Information coordinator. It is unknown as to whether

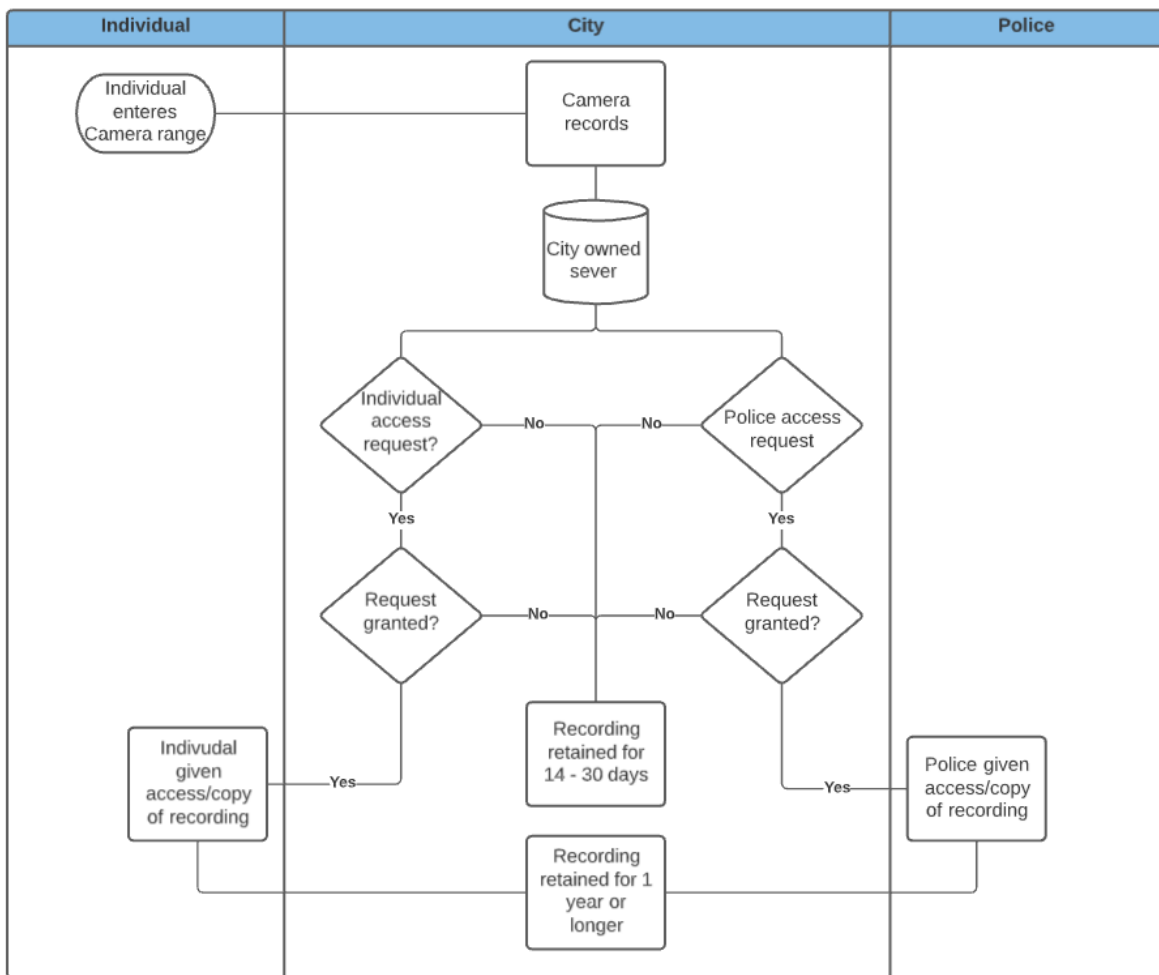
⁴ Policy Governing the Use of Video Surveillance Equipment in City of Cambridge Workplaces.

these audits have been regularly conducted for each of the Control Documents (as listed in section 3.1). This has been logged as risk 2 in section 7.

As per the Control Documents, recordings are kept for 14 to 30 days (depending on the City Facility) if no access request has been made for the recordings. In cases where an access request has been made by either an individual or police, the recordings will be retained for a year or longer as appropriate.

The City Facilities maintain and store any recordings on servers located at their facility and are responsible for the administrative and physical privacy and security considerations. This will be discussed in greater detail below.

The business process is depicted below:



2.2. Stakeholders

The following are the key stakeholders for the City of Cambridge surveillance camera program.

Stakeholder	Description
The City of Cambridge	As will be discussed in detail in section 5.1, per section 11 of the <i>Municipal Act</i> the City may provide any service or thing that the municipality considers necessary or desirable for the public. The City, in conjunction with police and the public advisory committee have determined a need for cameras. The City owns and operates all the camera systems on City property.
Individuals and Cambridge Businesses	Individuals and local businesses are key stakeholders in the surveillance camera program. Public consultations held prior to the installation of the Downtown Core camera.
Waterloo Regional Police	It was reported that the Waterloo Regional Police strongly advocated for the presence of cameras.

3. System Description

3.1. Camera Locations

There are surveillance Cameras located throughout the City. The known camera systems and locations are detailed in the chart below. It is also relevant to note that:

- “Live monitoring” refers to the live (real time) camera feed being available on a monitor, though does not necessarily imply that there is a designated employee with the sole responsibility of monitoring the cameras.
- All location Control Documents state that a Notice of collection will be posted to make individuals aware that there is camera surveillance in the area. The notice will be discussed in detail below.
- All access logs (access to recorded footage) are maintained at the facility level, and are maintained on paper.
- Control Documents for “Parks Office Building / Maintenance Shop” and the “William E. Pautler Centre” could not be located.

Location	# of cameras	Policy	Live monitoring	Camera move/zoom	Record Time	Recording Retention	System
Allen Reuter Centre 507 King St E	6	ARC Control Document	Yes	No	The cameras operate during regular business hours.	Recordings will be overwritten every 14 days (the system has a 14 day memory loop). ARC CD silent on accessed footage.	Langs
Beverly-Wellington Street Parking Lot	17	Beverly Lot Control Document	Yes	The view on these monitors can be controlled and selected by security personnel. Security personnel can control the zoom by means of a joystick or a mouse	Not expressly stated in the CD, however it is reasonable to assume the recording is ongoing.	Recorded data will be retained for 30 days. Accessed footage will be retained no less than one (1) year.	Symphon y

				located at the security station and in the office of the Buildings Operations Officer. The cameras can also be controlled using a web-based application through password-controlled access by the Corporate Property Manager and by Manager of Technology Services Support.			
Cambridge Downtown Core Area		Surveillance Cameras in the Downtown Core Area Policy	Yes	No.	Cameras will record activity in the public areas for 24 hours a day, 7 days a week.	In cases where the surveillance system records activities have been accessed the appropriate section of the recording will be copied to suitable media and stored in a separate secure location for a period of no less than one (1) year or a longer appropriate length of time	Gentec
Cambridge Youth Soccer Centre 745 Fountain St N	10	Youth Soccer Center Control Document	No	No	Ongoing. Recording activated via motion sensor.	Recorded data will be retained for approx. 14 days. Accessed footage will be retained no less than one (1) year.	Unknown
Civic Square	33	Civic Square Control Document	Yes.	Security personnel can control the pan/swivel/tilt cameras by means of a joystick or a mouse located at the security station and in	Ongoing	Recorded data will be retained for 30 days or until storage capacity is reached.	Symphony

				<p>the office of the Building Operations Officer.</p> <p>The pan/swivel/tilt cameras can be controlled using a web-based application through password-controlled access by the Corporate Property Manager and by Manager of Technology Services Support</p>		<p>Accessed footage will be retained no less than one (1) year.</p>	
David Durward Centre	4	David Durward Control Document	Yes	No	Not expressly stated in the CD, however it is reasonable to assume the recording is ongoing.	<p>Recorded data will be retained for approx. 14 days.</p> <p>The CD is silent on accessed footage.</p>	Honeywell
Duncan McIntosh Arena 200 Christopher Dr	16	Duncan McIntosh Arena Control Document		No	Ongoing. Recording activated via motion sensor.	<p>Recorded data will be retained for 2 weeks or until storage capacity is reached.</p> <p>Accessed footage will be retained no less than one (1) year.</p>	Unknown
George Hancock Pool 115 Glenmorris St	1	Control Document	Yes	No	Ongoing. Recording activated via motion sensor.	<p>Recorded data will be retained for 1 week or until storage capacity is reached.</p> <p>Accessed footage will be retained no less than one (1) year.</p>	Unknown

Hespeler Memorial Arena 640 Ellis Rd W	16	Hespeler Area Control Document	Yes	No	Ongoing.	Recorded data will be retained for 2 weeks or until storage capacity is reached. Accessed footage will be retained no less than one (1) year.	Unknown
John Dolson Centre 212 South St	11	John Dolson Control Document	Yes	No	Ongoing. Recording activated via motion sensor.	Recorded data will be retained for 1 week or until storage capacity is reached. Accessed footage will be retained no less than one (1) year.	Unknown
Mount View Cemetery 80 Blenheim Rd	3	Mountainview Cemetery Control Document	No	No	Ongoing. Recording activated via motion sensor.	Recorded data will be retained for 1 week or until storage capacity is reached. Accessed footage will be retained no less than one (1) year.	Unknown
Parklawn Cemetery 750 Fountan St. N	2	Parklawn Cemetery Office/Chapel Control Document	No	No	Ongoing. Recording activated via motion sensor.	Recorded data will be retained for 1 week or until storage capacity is reached. Accessed footage will be retained no less than one (1) year.	Unknown
Parks Office Building / Maintenance Shop 247 Elgin St. N	8	None located	Unknown	Unknown	Unknown	Unknown	Unknown

The Kinsmen Soper Park Pool 41 Marion Way	1	The Kinsmen Soper Park Pool Control Document	Yes	No	Ongoing. Recording activated via motion sensor.	Recorded data will be retained for 1 week or until storage capacity is reached. Accessed footage will be retained no less than one (1) year.	Unknown
W.G. Johnson Centre / Ted Wake Lounge 31 Kribs St	10	Johnson Center Control Document	Yes	No	Ongoing.	Recorded data will be retained for 1 week or until storage capacity is reached. Accessed footage will be retained no less than one (1) year.	Unknown
William E. Pautler Centre 1145 Concession Rd	4	None located	Unkn own	Unknown	Unknown	Unknown	Unknown

There are a number of unknowns relating to the City Facilities cameras. For 11 of the facilities, the type of camera system used is not known or is not documented, and for 3 of the facilities the technical capabilities of the camera to move is unknown. This presents a risk to the City, as there is missing information related to the technical capacity of the systems (e.g., zoom capability), the security considerations, and contractual agreement that the City may have with the vendor(s). This limits the opportunity for a fulsome privacy review. This lack of information has been logged as risk 3 in section 7.

4. Information Management

4.1. System Access Controls

Downtown Core Area Cameras

The Downtown Core Area is covered under two different surveillance systems: Symphony and Gentec. Both systems are maintained on the City servers located in a secure section of City Hall. Access to these systems is restricted to authorized personnel.

Under the *Surveillance Cameras in the Downtown Core Areas Policy* access to the recordings is restricted to:

- The Director of Economic Development,
- The Manager of Technology and Support Services,
- The Freedom of Information Coordinator or designate, and
- The Corporate Property Manager.

Under the Policy, the viewing of recordings is “only permitted for purposes compatible with the original purpose for the installation of the surveillance system. Approved viewing of the recorded information must be conducted in private and in the presence of authorized persons only”. All instances in which footage is accessed or viewed must be recorded in the access log (as described in the section below).

Technically, access to the surveillance systems (including recorded footage) is controlled via unique log-in credentials for each user. Login credentials for the system are assigned by the City’s facilities department and required managerial approval.

City Facility Camera

The remaining cameras are stand-alone systems which are not stored on the servers at City Hall. In these instances, the surveillance systems and recordings are managed at the facility level and under the Control Document specific to that facility. There is common language used throughout the Control Documents, including the section related to the access to recordings.

The Control Documents list those who are permitted to access recordings. This list varies by facility however, each Document lists the following:

- Senior management personnel for the facility (e.g., the president or vice president of the Cambridge Youth Soccer Association or the Director of Arenas);
- Commissioner of Community Services Department or relevant departmental supervisory staff;
- Senior City Management or senior Human Resources, or
- Waterloo Regional Police when conducting an investigation.

Given the various different systems used throughout the City, there is no standard understanding on how login credentials for access to the systems are authenticated and created. Though the Control Documents detail the roles which are permitted to have access to camera recordings there is no standard written policy or procedure.

The lack of standardization in access to recordings presents a risk to the City. In its current state each facility maintains their own Control Document and, while they use common language across the different locations, there is room for customization which may put the facility offside in regards to legislation or best practice. The lack of a standard policy may also create confusion amongst City employees and individuals or police making a request for access to footage.

The City does not currently have an Access Policy or Acceptable Use Policy which governs the PI under their custody or control. It is recommended that the City enact a standard Surveillance Camera policy, which includes a discussion on how the system and recordings are accessed.

The above has been logged as risk 4 section 7 of this document.

4.2. Logging and Auditing

In accordance with the *Surveillance Cameras in the Downtown Core Areas Policy*, logs are required to be kept on all access to surveillance camera recordings. The logs must include the following information:

- The date of access;
- The person accessing the recording, and
- The reason for accessing the recording.

In the event that recorded footage must be released in relation to a subpoena, search warrant, summons or other order of the courts or a quasi-judicial tribunal, a digital copy of the original recording will be provided. All access, disclosure, and copies of surveillance footage must also be entered into the log.

The *Surveillance Cameras in the Downtown Core Areas Policy*, does not apply to all surveillance cameras in the City. Each City facility has their own control document which outlines logging requirements. The language is largely standardized throughout the various City facilities, and reads:

7.1 A log will be kept to record access to the recorded information. An entry will be made each time the recorded information is consulted or copied. The log entry will note the person(s) accessing the recorded information and the reason for access.

7.2 Recorded information must be released if the information is subject to a subpoena, search warrant, summons or other order of the courts or a quasi-judicial tribunal. In these cases, a digital copy of the information on the recording system's hard drive will be provided. A second copy will be made for use by city staff or agents involved in the investigation. All actions taken in response to a subpoena etc. including the information that a copy was made will be entered into the log. A copy of the log entry will be filed with this document.

The Facility Camera systems are each governed under their location Control Document (as outlined above). Though each Control Document is different, each has a section titled "Logs" in which the process and expectations are defined. The log section states:

A log will be kept to record access to the recordings. An entry will be made each time the recordings are consulted or any a copy is made of any part of them. The log entry will note the person(s) accessing the recordings and the reason for access.

For the surveillance systems within both the City Facilities and the Downtown Core Area, the logs are not maintained electronically and there is no known electronic access log functionality. Though the City meets the legal base requirement for logging, the lack of electronic logging could affect the accuracy in which access to the footage is recorded. Though there is no legislative risk associated with the paper log, it is still recommended that the City further review the functionality of the surveillance systems to ascertain if a standard system and electronic access logs are feasible.

In the absence of an electronic access log, it is recommended that the City create and use a standard paper user access log template across all facilities, and include access logging within a standardized camera policy.

5. Privacy Analysis

5.1. Provincial Statutes

Municipal Freedom of Information and Protection of Privacy Act ("MFIPPA")

As a Municipality located on Ontario, the City of Cambridge is subject under MFIPPA in relation to the collection, use, disclosure, and right of access of Personal Information ("PI"). Under section 2(1) of the Act"

"institution" means,
(a) a municipality,

Under the surveillance camera program, the City will collect, use, and disclose the PI of identifiable individuals. PI is defined in section 2 of the Act as "recorded information about an identifiable individual", which would include information relating to "race, national or ethnic

origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual". These data elements could reasonably be collected via the cameras.

For further certainty, the Act's definition of a "record" includes "a film, a microfilm, a sound recording, a videotape".

Pursuant to section 28(2) of MFIPPA:

No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

Pursuant to section 28(2) as the cameras must be 1) lawfully authorized activity and 2) necessary for proper administration of the City.

Lawfully Authorized

The lawful authorization stems from section 11 of the *Municipal Act* ("MA") which states that:

A lower-tier municipality and an upper-tier municipality may provide any service or thing that the municipality considers necessary or desirable for the public, subject to the rules set out in subsection (4).

The City's lawfully authorized activity is the operation of the City, which includes maintaining the safety and security of municipal facilities (e.g.; parking lots, streets, recreation facilities, cemeteries, and trails) which can reasonably be considered both necessary and desirable for the public.

Necessary for the Proper Administration of the City

The collection of PI via surveillance cameras was deemed necessary for the proper administration of the City by Cambridge City Council. The City, in conjunction with the Police, determined that the cameras were necessary to address the issue of public safety in the Downtown Core Area. There is no documentation related to the decision to conduct camera surveillance in the City Facilities.

There is limited documentation available regarding how the determination that cameras were necessary was made. For the Downtown Core Area cameras, it is known that the City was reliant on police opinion, the Ambassador program, and a committee comprised of municipal officials, business owners, and police, and that the cameras are for "public safety". Documentation from these committee meetings were not available for review for this PIA.

The City does not have a record of the advice, guidance, or requests made by police in regards to setting up camera surveillance. During the PIA process, the City inquired with the Waterloo Regional Police regarding what information was shared or advice given during these discussions, however the police declined to provide this information.

Publicly available police statistics for the Cambridge area does show an increase in requests for police response to certain types of issues. It is relevant to note that these numbers do not

specify if an investigation was opened or if charges or fines were laid. The table below outlines the percentage change in calls between 2015 and 2019. A more detailed chart can be found at Appendix B.

Call Category	Change 2015-2019	Description
Abandoned Vehicle	97% decrease	Calls related to abandon vehicle decreased 86% in 2018. This drop correlates with the camera installation. ⁵
Break and Enter	111% increase	Rates of B&E related calls have increased gradually since 2017.
By-Law Complaint	68% decrease	By-law complaints have been decreasing since 2018.
Graffiti	500% increase	Graffiti calls have increased each year since 2015, with the exception of 2018, in which there was 92% drop. This drop correlates with the camera installation.
Drugs	58% increase	With the exception of a small drop in 2017, call related to drugs have increased.
Indecent Acts	300% increase	Although the change between 2015 and 2018 shows an increase, in 2017 there was a 20% decrease followed by a 75% decrease in 2018. This drop correlates with the camera installation.
Injured/Sick Person	2039% increase	In 2018 there was 3% decrease in calls related to the injured or sick persons, but an increase in all other years since 2015.

Through the publicly available statistics we can determine there was a rise in some categories of calls made to police which may have contributed to the decision to implement surveillance cameras.

Although there may be a strong case for the necessity of the camera, the lack of documentation may limit the ability for a fulsome discussion related to the necessity of these surveillance cameras. By extension, this may cast doubt on the City's adherence to section 28(2) of MFIPPA.

This lack of certainty and transparency represents a high risk to the City. There is a risk that the City is offside section 28(2) of MFIPPA. This has been logged as risk 5 in section 7.

5.2. Contracts and Agreements

In the course of conducting this analysis, one surveillance camera related agreement was located. This System Service and Maintenance Agreement is between Alliance Technology Services Inc ("Alliance") and the City. It is unknown as to whether the City entered into a contractual relationship with any of the other surveillance camera service providers (e.g.

⁵ It is relevant to note that while the drops in calls to police may correlate with the increase camera surveillance there is no available documentation or information that proves causality.

Symphony or Honeywell) for the provision of services or maintenance not covered under the Alliance Technology Services Contract.

This represents a risk to City, as there may be unknown contractual relationships with unknown parties. Additionally, the privacy and security considerations present within the missing contracts cannot be reviewed for compliance with law and existing City policy. This has been logged as risk 7 in section 7.

Alliance System Service and Maintenance Agreement (“Alliance Agreement”)

This Agreement was in force between July 2, 2019 and June 30, 2020. It is unknown as to whether the terms were extended either by replacement or amendment to the Agreement.

The Agreement outlines the roles and responsibilities of Alliance and the City. This includes a section related to the confidentiality of any information Alliance may have access to in the course of their duties:

18. Confidentiality.

The performance of installation and service requires access to confidential information from the Client such as, floor plans, contact information, etc. The Company is certified by the Underwriters Laboratories Canada (ULC) and all staff operate within strict Confidentiality and Privacy guidelines. Any confidential documents given to the Company will not be disclosed to any third party without written permission from the client.

It is not known which camera systems are covered under this agreement. The expiry and the unknown scope of the Agreement has been logged as risk 6 in section 7.

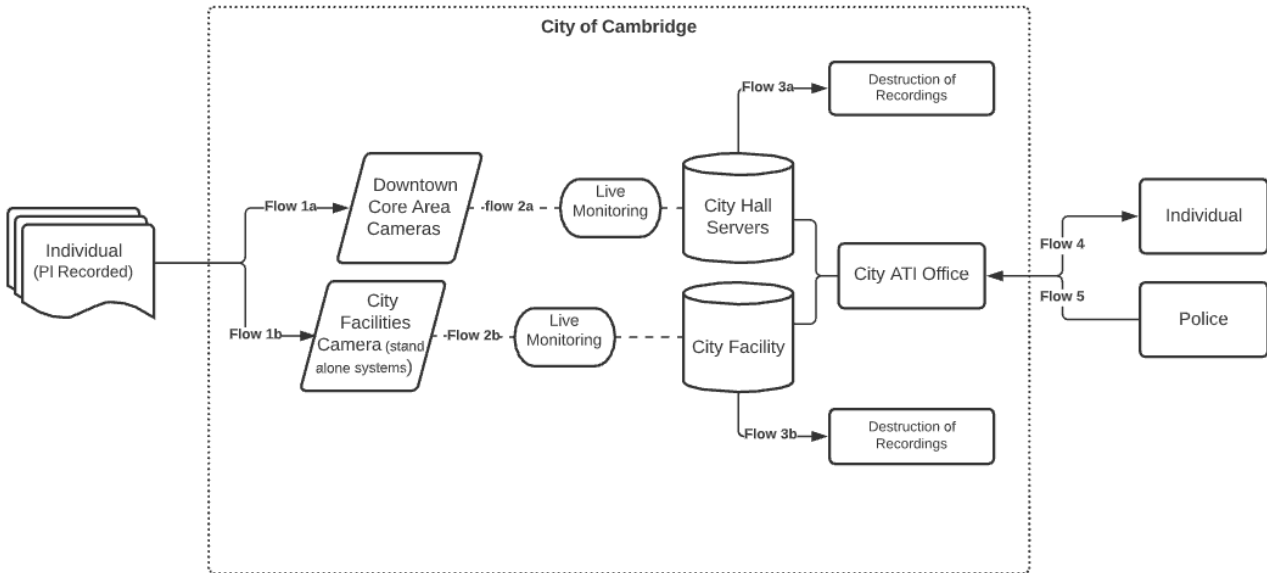
Staff Agreements

At the time of drafting, there is no staff confidentiality agreement or pledge of confidentiality signed by City employees. The City’s Freedom of Information Office and Privacy Officer (the City Clerk) are currently working with the City’s legal department to create and implement a Confidentiality Agreement to be signed by all staff.

The current lack of confidentiality agreement has been logged as risk 8 in section 7.

5.3. Dataflow and Legislative Authority

This section will review in detail the legislative authority for the actions undertaken by the City in connection to the surveillance camera program. A dataflow diagram and description chart can be found below.



#	Description	Purpose	Legislative Authority
1a 1b	PI is collected from the individual as they come into range of a camera in the Downtown area or a City Facility. A Notice of camera surveillance is posted.	PI is collected by the City to ensure to ensure the safety of the residents and visitors; deter unsafe activities; deter loitering on municipal streets and around public buildings; and contribute to the Cambridge Core Area revitalization.	MFIPPA s. 28(2) MA s. 11 MFIPPA s. 29(2)
2a 2b	The PI is used by City employees to monitor for the purposes of public safety. Note: Only some cameras have live monitoring by an on-duty security staff.	As above, the purpose is to ensure the safety of residents, visitors and staff. The PI was collected by the City for the purpose of ensuring safety, the use of the PI is consistent with this collection.	MFIPPA s. 31(c) An institution shall not use personal information except for a purpose for which the information may be disclosed to the institution under section 32 (...) of FIPPA FIPPA s. 32(c) An institution shall not disclose personal information except for the purpose for which it was obtained or compiled or for a consistent purpose;

3a 3b	<p>Surveillance camera recordings that have not been used/accessed by Police or an individual will be retained for 14-30 days.</p> <p>Camera recordings that have been used/accessed will be retained in a separate secure location and retained for at least 1 year.</p>	<p>In accordance with the Act, PI that has been used will be retained for one year to permit the individual time to make a request, and to ensure that data is not held indefinitely.</p>	<p>MFIPPA s. 30(1)(4) O.Reg 124/15, S. 5</p>
4	<p>An Individual may make a request to the City for access to surveillance camera footage. The City may collect PI about the requestor to fulfil the request.</p>	<p>An individual has the right to request access to information held about them by an Institution under MFIPPA. The City may be required to collect PI from the requestor to fulfil the request.</p>	<p>MFIPPA s. 4(1) MFIPPA 36(1) MFIPPA s. 28(2)</p>
5	<p>The City may disclose PI when requested by the Police.</p>	<p>The City may disclose PI to the Police for the purposes of aiding an investigation or, if there is a reasonable belief that an offense has been committed.</p>	<p>MFIPPA s. 32(g)</p>

6. Privacy Principles

6.1. Principle 1 – Accountability

An organization is responsible for the personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance. Organizations shall implement policies and practices to give effect to the principles.

The City has a designated Privacy Officer who is accountable for the organization's compliance with applicable privacy legislation, the 10 fair information principles, and City policy and procedure.

While the City does have a standard Privacy Policy (see Appendix E), this Policy does not include reference to the ability of an individual to make a complaint to the privacy officer, nor does it provide the contact information for the privacy officer or the Ontario Information and Privacy Commissioner's office. This has been logged as risk 9 in Section 7 as it represents non-compliance with best practice.

It is relevant to note that though the Privacy Policy does not list the required information, the signs posted publicly to notify individuals of the surveillance does include the contact information for the City Clerks Office.

As the City works to develop its privacy management program in respect to its surveillance cameras, it is recommended that the following be created to adhere to best practice:

- Individual Access (Access to Information Request) Policy and Procedure
- Employee Appropriate Use and Access Policy
- Records Correction Policy and Procedure
- Complaint Policy and Procedure
- Privacy training

6.2. Principle 2 – Identifying Purposes

Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information, they need to collect to fulfil these purposes. Depending upon the way in which the information is collected, this can be done orally or in writing.

The City's surveillance cameras collect PI from individuals. Pursuant to section 29(2) of MFIPPA, the City is required to give individuals notice of this collection.

Notice to individual

(2) If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,

1. the legal authority for the collection;
 - (b) the principal purpose or purposes for which the personal information is intended to be used; and
 - (c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection

The posted Notice (below) fulfils the above requirements, as it includes the legal authority for collection (MFIPPA), the purpose for collection (promotion of safety), and where to go in the event of questions or concerns (the City Clerk's office).



6.3. Principle 3 – Consent

Consent is typically required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent is not required.

Consent is not available as a source of authority for the collection of personal information under MFIPPA.

Section 31(1) of MFIPPA limits how PI may be used once it has been lawfully collected, in this case, under section 28(2) of the Act. As a general rule, the Act prohibit the use of PI unless 1) the institution obtains consent from the individual or 2) the personal information is used for the purpose for which it was obtained or compiled, or for a consistent purpose.

A “consistent purpose” is defined in section 33 of MFIPPA as a use of personal information that the individual might reasonably have expected at the time of collection.

In the context of the City’s camera surveillance, this means that the City may only use personal information collected by surveillance cameras for the purpose of the surveillance program or for a consistent purpose. This is supported by the *Surveillance Cameras in the Downtown core Areas Policy* which states:

The objectives of video surveillance systems are to ensure the safety of the residents and visitors; deter unsafe activities; deter loitering on municipal streets and around public buildings; and contribute to the Cambridge Core Area revitalization.

And

Use of video recordings - The information collected through video surveillance is used only for the purposes of contributing to the safe environment of the Cambridge Core Area, deterring unsafe activities and assisting as one of the components of Cambridge Core Area revitalization.

The Control Documents for the City Facilities uses common language surrounding the appropriate use of camera recordings. The Documents state that:

Use of the recordings is limited to post-incident evidentiary purposes but the Manager of Technology Services Support or other Tech Services staff designated by the Manager of Technology Services may view the recordings at the request of the Corporate Property Manager as needed for support purposes.⁶

The use described above is consistent with the purpose for collection of the PI, namely, the promotion of safety.

Furthermore, it is specifically stated within the Control Documents that recordings are not to be used for the purposes of employee evaluation:

It is understood that should an image of city employees appear on the monitor the information will not be used for the purposes of employee evaluation, for discipline or to investigate public complaints concerning staff. This statement does not extend to any evidence of criminal acts or acts with malicious intent by staff members captured by the surveillance system. This provision applies to contract staff as well as to city employees.⁷

Although consent for the initial collection of PI is not required, the City has the legal authority to collect the information and use it for a consistent purpose.

⁶ Civic Square Control Document, page 5

⁷ Civic Square Control Document, page 5

6.4. Principle 4 – Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified.

In accordance with the limiting collection principle the City has made the following decisions regarding the surveillance cameras in the Downtown Core. The Downtown core cameras are:

- Stationary and point at public areas;
- Located on property owned by the city or the region;
- Restricted to prohibit the viewing of locations not intended to be monitored (e.g., staff offices), and
- Prevented from looking through windows or areas where higher levels of privacy are expected (e.g., public washrooms).

In some City Facilities the cameras have the technical capability to swivel, pan, and zoom. For other City Facilities their incomplete information on the camera systems and capabilities. There is no standard policy governing the use of the camera movement capabilities. This, coupled with the incomplete information surrounding the technical capabilities of the cameras presents a risk of over collection of PI. This potential over collection has been logged as risk 10 in section 7.

It is relevant to note that the Downtown Core and City Facilities cameras do not have the capability to capture or record audio or other sensory information (e.g., heat).

6.5. Principle 5 – Limiting use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes. Organizations using personal information for a new purpose shall document this purpose

Limiting Use

As discussed above in Principle 3 – Consent, the City may only use personal information collected by surveillance cameras for the purpose of the surveillance program or for a consistent purpose.

Limiting Disclosure

The City does not disclose a recording of an individual except as permitted through MFIPPA. As per the *Surveillance in the Downtown Core Area Policy*, the City will disclose PI collected through surveillance cameras in the following situations:

1. **Public requests for disclosure** - Any person may make a written request for access to video records created through a video surveillance system through the freedom of information process. Access may depend on whether there is a justified invasion

- of another individual's privacy and whether any exempt information can be reasonably severed from the record. (Through appropriate request form)
2. **Internal requests for disclosure** – City employees or consultants may request a copy of a video recording if it is necessary for the performance of their duties in the discharge of the corporation's function.
 3. **Law enforcement requests** - The City may disclose a copy of a video recording to a law enforcement agency where there are reasonable grounds to believe that an unlawful activity has occurred and has been captured by the video surveillance system in accordance with section 32. (g) of MFIPPA.(through appropriate request form)

There is a request form for both public (individual) requests, as well as law enforcement requests. These forms have been appended to this PIA as Appendix C and D

Limiting Retention

Under the City's *Surveillance in the Downtown Core Area Policy*, a distinction is made between the retention of recordings that have been accessed via a public or law enforcement request, and recordings that have not. The Policy states that recordings that have not been accessed are considered transitory:

Video that has not been requested by the public, City employees or law enforcement agencies within the maximum retention period is considered transitory and is automatically erased by being overwritten.

These transitory records are held for 30 days until they are overwritten.

Images are recorded on digital video servers with a storage area network (SAN) located in the server room. Recordings are retained for one month (30 days) or until storage capacity is reached. The data is then overwritten (...)

Recordings may be retained for a longer period of time for the purposes of insurance, liability, law enforcement or other similar issues

Regarding recordings that have been accessed, in accordance with section 30(1) of the Act, and section 5 of O. Reg 823 PI will be retained for one year:

An institution that uses personal information shall retain it for the shorter of one year after use or the period set out in a by-law or resolution made by the institution or made by another institution affecting the institution, except if,

- (a) the individual to whom the information relates consents to its earlier disposal;
- or
- (b) the information is credit or debit card payment data. O. Reg. 124/15, s. 1.

The above legislative requirement is codified within the City's *Surveillance in the Downtown Core Area Policy* which states that:

In cases where the surveillance system records activities that relate to an insurance, liability, law enforcement or other similar issue, the appropriate section of the recording will be copied to suitable media and stored in a separate secure location for a period of no less than one (1) year or a longer appropriate length of time.

The Control Documents also include reference to the limiting of data retention. The Control Documents state that:

In cases where the surveillance system records activities that relate to an insurance, liability, law enforcement or other relevant issue, the appropriate section of the recording will be copied to suitable media and stored in a separate secure location for a period of no less than one (1) year or for the period determined by its secondary use.

As discussed above, it is recommended that the City create a standard surveillance camera policy which applies to all surveillance camera in the City.

6.6. Principle 6 – Accuracy

Personal information must be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual.

The PI collected through the surveillance cameras is not used by the City to make decisions on behalf of the individual, and unless requested by law enforcement or the individual the recordings are not retained. Information collected through the surveillance cameras do not form and are not included within any other records about the individual held by the City.

Though it is technologically possible for recorded footage to be altered the City does not have the capacity or technology to alter video recordings.

6.7. Principle 7 – Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

As discussed above under Principle 5 the *Surveillance in the Downtown Core Area Policy*, limited discloser of PI collected through surveillance cameras to the following situations:

1. **Public requests for disclosure**
2. **Internal requests for disclosure.**
3. **Law enforcement requests**

In order to safeguard PI contained within the recordings, the Control Documents for the various City facilities require that a log be kept of all access and disclosure of records. This requirement is also present within the *Surveillance Cameras in the Downtown Core Areas Policy*.

Additionally, as described in section 4.1 of this PIA, there are policy and administrative restrictions on what role may access the recordings and for what purpose.

Given that each Control Document is different, there is no standardized approach or guidance on which roles may access the recordings. This lack of standardization presents a risk to the City, and has been logged under risk 1, 2, and 4 in section 7.

6.8. Principle 8 – Openness

An organization shall make readily available to individuals' specific information about its policies and practices relating to the management of personal information. Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

As referenced above, a Notice is posted throughout the areas in which camera surveillance is utilized. This Notice includes the contact information of the City Clerk, who is the key contact in the event of questions relating the surveillance cameras.

The *Surveillance in the Downtown Core Area Policy* is available on the City's public facing website. The Policy is located within the page describing the Core Area cameras, and includes a list and map of camera locations. The website invites individuals with questions to contact the Economic Development division, and provides a link to their contact form.

Though the public facing website provides a great deal of information on the Downtown Core Area Cameras, there is no information pertaining to the surveillance cameras located within City Facilities.

The public facing website does not have privacy specific page, however, the Freedom of Information page does provide some information on the protection of privacy:

"In addition to providing individuals with access to municipal records, the Act also requires the City of Cambridge to protect the personal privacy of individuals. Personal information is collected and used by the City for very specific purposes, which are identified at the time of collection. Your personal information will not be used for any other purpose than identified at the time of collection, nor disclosed in any circumstance, except as permitted by the Act. If you feel your personal information has

been misused or disclosed in a manner that is not consistent with the Act, please contact the City Clerk's Office"⁸


This section provides some information on the protection of privacy and includes information on where and how to make a privacy complaint, however the City's Privacy Policy is not posted on the website nor is the contact information for the Privacy Officer (City Clerk) easily accessible. This has been logged as risk 11 in section 7.

6.9. Principle 9 – Individual Access

Upon request, an individual must be informed of the existence, use and disclosure of his or her personal information and must be given access to that information. An individual must be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Individuals are able to request access to the information (recordings) collected about them via the surveillance camera system. While there is no formal policy or procedure (as has been mentioned above and logged as risk 4 in section 7) there is an existing form in which individuals can make their requests.

To make a request, the individual must complete the form (see Appendix C) and provide enough information for the FOI Coordinator to fulfil the request. Recordings of individuals are not included within other records held by the City, and therefore must specifically be requested on the form (e.g.; a request for "all information held about me by the city" would not return camera recordings unless specifically requested).



Access/Correction Request
Freedom of Information and Protection of Privacy
 A \$5.00 application fee is required for ALL requests made under the
Municipal Freedom of Information and Protection of Privacy Act.
 Cheque or money orders should be made payable to the City of Cambridge.

Request for: <input type="checkbox"/> General Records <input type="checkbox"/> Access to Own Personal Information <input type="checkbox"/> Correction to Own Personal Information		Name of Institution request made to: <div style="text-align: center; font-weight: bold; font-size: 1.2em;">CITY OF CAMBRIDGE</div>	
If request is for access to or correction of your own personal information records please indicate last name appearing on records <input type="checkbox"/> Same as below, or: _____			
Last Name: _____		First Name: _____	
Mailing Address: _____			
City / Town: _____		Province: _____	Postal Code: _____
Phone Numbers: (Day): _____ (Mobile): _____			
Email Address: _____			
** Please note that the use of personal contact information will only be used as a communication tool related to this request. Records packages will <u>ONLY</u> be available via Regular Mail or for Pick Up.			
Please provide a detailed description of requested records, personal information records or personal information to be corrected. (If you are requesting access to, or correction of your personal information, please identify the personal information bank or record containing the personal information, if known). (Please use the back of this form if additional space is required). _____			

⁸ <https://www.cambridge.ca/en/your-city/Freedom-of-Information.aspx>

As noted on the City's website:

As per the provisions of MFIPPA, the has thirty (30) calendar days (including weekends and statutory holidays) from the date a completed FOI request has been received with the applicable fee, to provide the information to the requester and/or a decision regarding the request.

There are circumstances where the Office of the Clerk may require an extension. If an extension is required, the Clerk will notify you in writing.

The website also details the estimated fees associated with a request. The City fee estimate's align with the fee estimates as included section 5.2 of O Reg 825:

MFIPPA Fees

The standard application fee is \$5.00 made payable to City of Cambridge; however, there may be additional fees depending on the nature and complexity of the request.

These include:

Search Time	\$7.50 per 15 minutes required to search and retrieve records
Preparation Time	\$7.50 per 15 minutes required to prepare records for release
Photocopying	\$0.20 per page
CDs/DVDs/USBs	\$10.00 each

Regarding the right to challenge the accuracy and completeness of the information, in the case of camera recordings which cannot be altered by the City, the request for correction cannot be granted.

6.10. Principle 10 – Challenging Compliance

An individual has the right to be able to address a challenge concerning compliance with the above to the designated individual or individuals with regard to the organization's compliance. Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

As noted above, the public facing website includes a statement on where to make a privacy complaint. The website states: "If you feel your personal information has been misused or disclosed in a manner that is not consistent with the Act, please contact the City Clerk's

Office.”⁹The website does not appear to include the contact information of the City Clerk, or reference to the Information and Privacy Commissioner. This gap in information has been logged as risk 11 in section 7. It is recommended that the City include the contact information for both the City Clerk and the Information and Privacy Commissioner on their public facing website.

⁹ <https://www.cambridge.ca/en/your-city/Freedom-of-Information.aspx>

7. Risk Assessment

In this assessment, 11 privacy risks were identified. Please note that for the purposes of this assessment, a gap in compliance with applicable laws, regulations, policies, or contracts will be referred to as a risk.

Risk Reference Table			
Impact	Likelihood		
	Low	Medium	High
Low	Very Low	Low	Very High
Medium	Low	Medium	High
High	Very Low	High	Very High

Status	Description
Inactive	The Risk is not active and does not require action at this time
Pending	The Risk is considered active and the identified mitigation(s) is pending
Initiated	The Risk is considered active and the identified mitigation(s) has been initiated.
Complete	The Risk is considered active and the identified mitigation(s) has been completed.

#	Privacy Risk / Threat	Likelihood	Impact	Risk Level	Mitigation Strategy	Status	Risk Level After Mitigation
1	It is unknown as to whether the <i>Policies Governing the Use Of Video Surveillance Equipment in City Of Cambridge Workplaces</i> document has been reviewed or updated since 2004.	M	H	H	It is recommended that the City enact a standard Surveillance Camera Policy, the use of camera surveillance to replace this Policy, the Downtown Core Area Policy and various Control Documents. A standardized approach will help ensure there is compliance with law and policy in the use of camera surveillance and access requests for recordings.	Pending	L
2	It is unknown as to whether the Control Documents for each City Facility are reviewed every two years as stated in the <i>Policies Governing the Use Of Video Surveillance Equipment in City Of Cambridge Workplaces</i> document.	M	H	H	It is recommended that the City enact a standard Surveillance Camera Policy, the use of camera surveillance to replace the various existing policies and Control Documents. This policy should include a standard audit and review schedule and procedure.	Pending	L

3	There is missing information on the systems used and the technical capabilities for a number of the City Facilities.	M	M	M	<p>The camera system information and technical capabilities of each camera system should be documented in a single document.</p> <p>The FOI office is currently in the progress of compiling this information.</p>	Initiated	L
4	The City does not currently have an Individual Access Policy (however there is an Access request form) or an Employee Acceptable Use Policy which governs the PI under its custody or control.	H	H	H	<p>It is recommended that the City enact a standard Surveillance Camera Policy, which includes guidance on how the system and recordings are accessed and by whom.</p> <p>It is further recommended that the City consider implementing an Acceptable Use policy for all PI (not just camera recordings).</p>	Pending	L
5	There is a risk that the City is offside section 28(2) of MFIPPA, as there is limited information available on how and why the decision to implement surveillance cameras was made.	H	M	H	<p>It is recommended that the City compile this information.</p> <p>The FOI office has been working towards this goal however has met significant roadblocks.</p>	Initiated	VL
6	The Alliance Agreement (section 5.2 of this PIA) expired on June 30, 2020.	M	M	M	Should the City wish to continue their relationship with Alliance, it is recommended they review and renew the signed Agreement.	Pending	L
7	It is unknown if the City has entered into other Agreements for the purchasing, use, maintenance or other considerations related to camera surveillance.	H	H	H	<p>It is recommended that the City compile this information and work towards a contract management system/process.</p> <p>The FOI office has been working towards this goal however has met significant roadblocks.</p>	Initiated	L
8	There is currently no staff confidentiality agreements or pledge of confidentiality signed by City employees.	M	H	M	It is recommended that the City create and implement a Confidentiality Agreement to be signed by staff, in keeping with best practice.	Initiated	VL

					<p>This agreement will ensure that staff are fully aware of their responsibilities when handling PI.</p> <p>Work on this document has begun.</p>		
9	<p>The City's current privacy policy does not include the following information:</p> <ul style="list-style-type: none"> • Individual's right to make a complaint • Contact information for the Privacy Officer • How to make a complaint to the Privacy Officer • Contact information for the IPC 	M	H	M	It is recommended that the City update its Privacy Policy to adhere to best practice principles.	Pending	VL
10	There is no standard policy governing the use of the camera movement capabilities. This, coupled with the incomplete information surrounding the technical capabilities of the cameras presents a risk of over collection of PI.	H	H	H	It is recommended that the City enact a standard Surveillance Camera Policy, which includes guidance on how the movement capabilities of cameras can be used, in what situation, and by whom.	Pending	L
11	City's Privacy Policy is not posted on the website nor is the contact information for the Privacy Officer (City Clerk) easily accessible.	M	H	M	It is recommended that the City add the Privacy Policy to the website, and include the contact information for the Privacy Officer or their office.	Pending	VL

8. Recommendations

Based on the results of the risk analysis, a number of recommendations have been developed to mitigate identified privacy risks, close any compliance gaps, and reduce to overall level of residual risk to an acceptable level. In addition, each recommendation has been assigned a Priority, to guide in the development of a Risk Treatment Plan.

Recommendation	Risks Mitigated	Residual Risk	Priority
Compile information related to how and why the decision to implement surveillance cameras was made.	5	Low	Medium
It is recommended that the City enact a standard Surveillance Camera Policy, the use of camera surveillance. Policy should include:	1, 2, 4, 10	Low	High

<ul style="list-style-type: none"> • Policy review schedule • Access audit schedule • Access permissions • Acceptable use of recordings • How movement capabilities of cameras can be used, in what situation, and by whom. 			
Compile information regarding any contracts or agreements that the City has entered into in relation to camera surveillance	7	Very Low	High
The camera system information and technical capabilities of each camera system should be documented in a single document.	3	Low	High
It is recommended that the City create and implement the following additional privacy considerations: <ul style="list-style-type: none"> • Records Correction Policy and Procedure • Complaints Policy and Procedure • Privacy training for all City staff 	General	Low	Medium
Consider implementing an Acceptable Use Policy for all PI (not just camera recordings).	4	Low	Medium
Create and implement a Confidentiality Agreement to be signed by staff, in keeping with best practice.	8	Very Low	Medium
Update the City Privacy Policy to include: <ul style="list-style-type: none"> • Individual's right to make a complaint • Contact information for the Privacy Officer • How to make a complaint to the Privacy Officer • Contact information for the IPC 	9	Very Low	Medium
Post the City's Privacy Policy on the public facing website, and include the contact information for the Privacy Officer and the IPC.	11	Very Low	Medium
Update or renew the Agreement with Alliance	6	Very Low	Low
If feasible, consider consolidating camera systems across the City and creating an electronic access log for recorded footage.	General	Low	Very Low

Appendix A – Risk Rating Methodology

This appendix describes how the risk ratings in this assessment were determined.

Likelihood	Risk Reference Table				
	Medium	Medium	High	Very High	Very High
	Low	Medium	Medium	High	Very High
	Low	Low	Medium	Medium	High
	Very Low	Low	Low	Medium	Medium
	Very Low	Very Low	Low	Low	Medium
Impact	Very Low	Low	Medium	High	Very High

Definitions for Impact ratings are as follows:

- **Very High:** There would be exceptionally grave consequences if the risk were to occur
- **High:** There would be very serious consequences if the risk were to occur
- **Medium:** There would be significant consequences if the risk were to occur
- **Low:** There would be low - marginal consequences if the risk were to occur
- **Very Low:** The consequences would be negligible if this risk to occur

Definitions for Likelihood ratings are as follows:

- **Very High:** This risk to privacy will almost certainly occur
- **High:** There is a very good chance that the risk to privacy will occur, particularly if there is a history of it having frequently occurred in this or similar environments
- **Medium:** There is a good chance that the risk to privacy will occur, particularly if there is a history of it having previously occurred in this or similar environments
- **Low:** It is very unlikely that this risk to Privacy will occur
- **Very Low:** This risk to privacy will almost certainly not occur

Appendix B – Publicly Available Police Generated Statistics

The following information relates to the type or category of call in which the police were contacted. This information does not denote whether a crime was committed, and investigation was opened, or charges laid.

	2015	2016	2017	2018	2019	2020	2021	Total Calls	Average Calls	Change 2015-2016	Change 2016-2017	Change 2017-2018	Change 2018-2019	Change 2015-2019
Abandoned Vehicle	32	3	7	7	1	9		59	10	-91%	133%	0%	-86%	-97%
Alarm	236	59	89	75	61	35		555	93	-75%	51%	-16%	-19%	-74%
Animal Complaint (Non By-law)	38	14	10	8	13	14		97	16	-63%	-29%	-20%	63%	-66%
Arrest	227	158	136	219	233	179		1152	192	-30%	-14%	61%	6%	3%
Assault	62	56	61	76	62	56		373	62	-10%	9%	25%	-18%	0%
Assist Other Service	119	23	24	47	38	29		280	47	-81%	4%	96%	-19%	-68%
Breach of Judicial Order	71	88	84	84	81	90		498	83	24%	-5%	0%	-4%	14%
Break and Enter	18	32	21	25	38	41		175	29	78%	-34%	19%	52%	111%
By-law Complaint	89	96	99	128	80	58		550	92	8%	3%	29%	-38%	-10%
Counterfeit Money	7	0	1	17	17	9		51	9	-100%	100%	1600%	0%	143%
Criminal Harassment/Stalking	3	1	1	3	1	0		9	2	-67%	0%	200%	-67%	-67%
Dangerous Condition	21	34	58	97	77	84		371	62	62%	71%	67%	-21%	267%
Dispute	63	61	70	64	63	87		408	68	-3%	15%	-9%	-2%	0%
Disturbance	94	107	159	225	151	119		855	143	14%	49%	42%	-33%	61%
Domestic Dispute	111	83	80	81	89	78		522	87	-25%	-4%	1%	10%	-20%
Domestic Other	21	30	24	19	33	27		154	26	43%	-20%	-21%	74%	57%
Driving Complaint	74	92	81	76	79	67		469	78	24%	-12%	-6%	4%	7%
Drugs	36	61	44	51	57	42		291	49	69%	-28%	16%	12%	58%
Elder Abuse	0	1	1	1	0	1		4	1	100%	0%	0%	-100%	0%
Escort	3	0	1	3	2	1		10	2	-100%	100%	200%	-33%	-33%
Fire	7	18	14	22	16	32		109	18	157%	-22%	57%	-27%	129%
Fraud - Financial Institution	2	4	5	3	2	2		18	3	100%	25%	-40%	-33%	0%
Fraud - General	16	23	18	25	24	19		125	21	44%	-22%	39%	-4%	50%
Fraud - Personal	3	4	2	1	2	3		15	3	33%	-50%	-50%	100%	-33%
Graffiti	0	3	48	4	5	0		60	10	300%	1500%	-92%	25%	500%
Human Trafficking	0	0	0	0	1	1		2	0	0%	0%	0%	100%	100%
Impaired Driver	1	11	11	5	15	2		45	8	1000%	0%	-55%	200%	1400%
Indecent Act	0	7	15	12	3	0		37	6	700%	114%	-20%	-75%	300%
Injured/Sick Person	18	215	311	396	385	34		1359	227	1094%	45%	27%	-3%	2039%
Intoxicated Person	2	68	48	55	29	2		204	34	3300%	-29%	15%	-47%	1350%
Liquor Offence	13	10	10	10	4	35		82	14	-23%	0%	0%	-60%	-69%
Mentally Ill	73	86	93	105	95	72		524	87	18%	8%	13%	-10%	30%
Missing Person	28	17	22	22	22	23		134	22	-39%	29%	0%	0%	-21%

Appendix C – Individual Access Request Form



Access/Correction Request

Freedom of Information and Protection of Privacy

A \$5.00 application fee is required for ALL requests made under the *Municipal Freedom of Information and Protection of Privacy Act*.
Cheque or money orders should be made payable to the City of Cambridge.

Request for: <input type="checkbox"/> General Records <input type="checkbox"/> Access to Own Personal Information <input type="checkbox"/> Correction to Own Personal Information	Name of Institution request made to: <h2 style="text-align: center;">CITY OF CAMBRIDGE</h2>
---	---

If request is for access to or correction of your own personal information records please indicate last name appearing on records ☐ Same as below, or: _____

Last Name:	First Name:
-------------------	--------------------

Mailing Address:

City / Town:	Province:	Postal Code:
---------------------	------------------	---------------------

Phone Numbers: (Day): _____ (Mobile): _____

Email Address: _____

**** Please note that the use of personal contact information will only be used as a communication tool related to this request.
Records packages will ONLY be available via Regular Mail or for Pick Up.**

Please provide a detailed description of requested records, personal information records or personal information to be corrected. (If you are requesting access to, or correction of your personal information, please identify the personal information bank or record containing the personal information, if known). (Please use the back of this form if additional space is required).

Note: If you are requesting a correction of personal information, please indicate the desired correction and, if appropriate, attach any supporting documentation. You will be notified if the correction is not made and you may require that a statement of disagreement be attached to your personal information.

Preferred method of access:	<input type="checkbox"/> Examine Original	Signature:	Date:
	<input type="checkbox"/> Receive Copy		

Personal information contained on this form is collected pursuant to Municipal Freedom of Information and Protection of Privacy legislation and will be used for the purpose of responding to your request. Questions about this collection should be directed to the City Clerk's Office of the Corporate Services Department @ 519-740-4680.

For Institution Use Only:		
Date Received:	Request Number:	Response Date:

[illegible]

Appendix D – Police Access Request Form



LAW ENFORCEMENT OFFICER REQUEST FORM DISCLOSURE OF PERSONAL INFORMATION

Corporate Services Department – Office of the City Clerk

The following information is being requested under section 32(g) of the Municipal Freedom of Information and Protection of Privacy Act (the Act) which provides for the disclosure of records containing personal information of an individual for the purpose of aiding an investigation with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

PART ONE: DETAILS OF REQUEST (To be completed by Law Enforcement Officer)

Department/Division which holds the information (if known):			
Information Requested (please describe):			
Occurrence/Investigation/Reference No.:	Review Original Documents: ____ Yes ____ No	Copies Requested: ____ Yes ____ No	
Name of Law Enforcement Agency:	Name of Law Enforcement Officer:	Badge/ID No.:	Telephone:
Signature of Law Enforcement Officer:		Date:	

PART TWO: INFORMATION/RECORD(S) DISCLOSED (To be completed by City Staff disclosing information/records):

Department/Division Contact Name:	Title/Position:	Telephone:
Information/Record(s)/File(s) Disclosed (please describe):		
Date Disclosed:		
Name of Staff Member:	Title/Position:	Telephone:
Signature of Staff Member:	Date:	

Appendix E – Cambridge Privacy Policy

City of Cambridge Privacy Policy

- The City of Cambridge is committed to protecting the privacy of any recorded personal information gathered by the city. The practices of the City of Cambridge related to the gathering and handling of personal information are designed to comply with the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act.
- Whenever City of Cambridge staff members collect personal information they will collect only the personal information that is needed to carry out the specific function for which the information is being gathered.
- The City of Cambridge will not share any personal information with any other organization or individual unless authorized do so by statute or with the consent of the person to whom the information relates. Within the corporation personal information will be made available only to those staff members who need the information to respond to inquiries or to otherwise perform their job functions. The city will endeavour to put safeguards in place wherever personal information is handled, including computer programs, to protect personal information from unauthorized access.
- The City of Cambridge will not use the personal information to create individual profiles nor will staff combine the personal information provided to the city with information from other electronic sources to create new databases. Nor will this information be provided to a third party for data base production except as permitted by statute or with the express permission of the person to whom the information relates.

City of Cambridge - Camera Inventory

Facility / Location	Municipal Address	No. of Cameras
Civic Campus		
Beverly Street Parking Lot	15 Beverly St	17
Bishop Street / Snow Dump Fill Station	1310 Bishop St	7
By-Law Enforcement Building	17 Cambridge St	3
City Hall Building	50 Dickson St	32
Civic Square	-	8
Civic Square Parking Long	40 Thorne St	10
Farmers Market	40 Dickson St	6
Historic City Hall Building	46 Dickson St	8
Market Square Lot	40 Dickson St	5
Galt Phase 1		
Main St at Water St	4 Water St N	1
Dickson Parking Lot	44 Main St	1
Main St and Ainslie St	60 Main St	1
Main St at Wellington St	5 Wellington St	1
Water St Lot 2 (West)	9 Water St	1
Water St Lot 2 (East)	9 Water St	1
Mill St Lot (West)	15 Lutz St	1
Main St Lot	119 Main St	1
Mill St Lot (East)	15 Lutz St	1
Pedestrian Bridge	75 Water St S	1
Galt Phase 2		
Pedestrian Bridge (E End)	56 Water St	1
Dan Spring Way Trail	Park Hill Dr W	1
Dan Spring Way Trail	Park Hill Dr W	1
Dan Spring Way Trail	Park Hill Dr W	1
Dan Spring Way Trail	Park Hill Dr W	1
Dan Spring Way Trail	Park Hill Dr W	1
Galt Phase 3 **Installation Pending		
Alley of Westminster that runs parallel to King	644 Duke St	1
Westminster Dr S	710 King St E	1
King and Westminster	105 Westminster Dr N	1
Westminster Dr N	105 Westminster Dr N	1
Church St S	780 King St E	1
Church and King	807 King S E	1
Lothar and King	863 King S E	1
King and Argyle	615 King St E	1
King and Dolph	112 Dolph St N	1
King St E beside Giant Tiger	927 King S E	1

City Facilities

Allen Reuter Centre	507 King St E	6
Cambridge Centre for the Arts	60 Dickson St	2
David Durward Centre	62 Dickson St	4
Duncan McIntosh Arena	200 Christopher Dr	16
William E. Paulter Centre	1145 Concession Rd	4
John Dolson Centre	212 South St	11
W.G Johnson Centre/Ted Wake Lounge	31 Kribs St	10
Hespeler Memorial Arena	610 Ellis Rd W	11
Cemeteries		
Parklawn Cemetery / Admin Office	750 Fountain St N	2
Mount View Cemetery	80 Blenheim Rd	3
Ed Newland Pool	515 William St	1
George Hancock Pool	115 Glenmorris St	1
The Kinsmen Soper Park Pool	41 Marion Way	1
Parks Office Building / Maintenance Shop	247 Elgin St N	8
Cambridge Youth Soccer Centre	745 Fountain St N	10
Works Depot	1310 Bishop St	18
Miovision Scout Unit	Transportation Division	1
FIRE - Apparatus - Rescue (R-31)	**Removed from Scope of PIA	0
Total Camera Inventory		231

POLICY TITLE	Surveillance Cameras in the Downtown Core Areas
CATEGORY	Administration
POLICY NUMBER	A09 ADM 004
DEPARTMENT	Corporate Services
POLICY AUTHOR	City Clerk
POLICY TYPE	City Policy
APPROVED BY	Council
EFFECTIVE DATE	09/18/2019
REVIEW DATE	09/01/2024

POLICY STATEMENT

The City of Cambridge recognizes the balance between an individual's privacy and the need to protect the safety and security of the public. In respecting this balance, the City is committed to integrating security best practices with the responsible use of technology. The City ensures that the information captured on video surveillance is maintained as private, confidential and secure, except or in situations outlined by this policy.

PURPOSE

The objectives of video surveillance systems are to ensure the safety of the residents and visitors; deter unsafe activities; deter loitering on municipal streets and around public buildings; and contribute to the Cambridge Core Area revitalization.

DEFINITIONS

Archive means the process of moving data that is no longer actively used to a separate storage device for long-term retention.

Cambridge Core Areas means the core areas as established by Maps 3, 4, and 5 in the City of Cambridge Official Plan (and attached in Schedule A), namely the Galt City Centre, the Preston Towne Centre, and Hespeler Village, respectively.

City means the Corporation of the City of Cambridge

Clerk means the City Clerk of the Corporation of the City of Cambridge.

Consistent purpose means personal information collected by the City of Cambridge used for the purpose for which it was collected or similar consistent purposes when carrying out City business. The individual to whom the information relates might reasonably expect the use/disclosure of their personal information for those consistent purposes.

Control (of a record) means the power or authority to make a decision about the use or disclosure of a record.

Custody (of a record) means the keeping, care, watch, preservation or security of a record for a legitimate business purpose. While physical possession of a record may not always constitute custody, it is the best evidence of custody.

Destruction is the physical or electronic disposal of records or data by means of disposing, recycling, deletion or overwriting. This also includes the destruction of records or data residing on computers and electronic devices supplied or paid for by the Corporation.

Digital video recording equipment means any type of video recording and reception equipment used as part of the video surveillance system.

Freedom of information process means a formal request for access to records made under the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Head refers to the City Clerk.

Information and Privacy Commissioner means the Information and Privacy Commissioner of Ontario (commonly referred to as the IPC). The IPC hears appeals of decisions made by Heads of institutions, issues binding orders, conducts privacy investigations, and has certain powers relating to the protection of personal privacy as set out in the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) means legislation that governs access to and the privacy of municipal records.

Personal information means recorded information about an identifiable individual, as outlined in MFIPPA.

Privacy breach means an incident involving unauthorized disclosure of personal information, including it being stolen, lost or accessed by unauthorized persons.

Record means information however recorded or stored, whether in printed form, on film, by electronic means or otherwise, and includes documents, financial statements, minutes, accounts, correspondence, memoranda, plans, maps, drawings, photographs and films; includes transitory records.

Retention period is the period of time during which a specific records series must be kept before records in that records series may be disposed of.

Service provider means a video service provider, consultant or other contractor engaged by the City in respect of the video surveillance system.

Video surveillance system means a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of individuals in public spaces or within City operated facilities.

AUTHORITY

The collection of personal information through video surveillance must adhere to the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). The policies, as attached, have been vetted by the Deputy City Clerk, Legal Services, the Information Privacy Commissioner of Ontario and the Region of Waterloo to ensure all appropriate adherences to applicable legislation.

SCOPE

This policy applies to all City of Cambridge employees, including full-time, part-time, casual, contract, volunteer and co-op placement employees.

Contractors and service providers are afforded the same rights and expectations as employees in this policy, while performing authorized activities for the City.

This policy applies to municipal video surveillance systems located in the Cambridge Core Areas.

This policy does not apply to covert surveillance used as an investigation tool for law enforcement purposes or in contemplation of litigation, which are under policy HRLS-270.020.

POLICY

The City of Cambridge is responsible for the video surveillance systems and maintaining custody and control of video records at all times on City property.

The collection of personal information through video surveillance is necessary for the proper administration of lawful municipal activities to ensure the safety of residents and

visitors, deter unsafe activities and loitering on municipal streets and around public buildings and to contribute to Cambridge Core Area revitalization.

Providing notice: Signs are posted at public access points to and within areas under video surveillance.

All attempts are made to ensure proper signage is posted at all locations using a video surveillance system.

Ownership: The cameras are owned by the City of Cambridge.

Camera placement: Where possible, all cameras that are adjustable or moveable are restricted to prohibit the viewing of locations not intended to be monitored. Cameras are prevented from looking through a window of an adjacent building or areas where a higher level of privacy is expected, such as private amenity space. Camera placement and diagrams are located within the **Control Document (Schedule B)**.

Only the Director of Economic Development (or designate) in coordination with the City Clerk, the Manager of Technology and Support Services, and the Corporate Property Manager may install, change or authorize a service provider or employee to install or change a camera's permanent setting.

Use of video recordings - The information collected through video surveillance is used only for the purposes of contributing to the safe environment of the Cambridge Core Area, deterring unsafe activities and assisting as one of the components of Cambridge Core Area revitalization.

Signage – Sign design is located in the Control Document as attached as Schedule B to this document. Further, wording for signage is as follows:

“To promote safety this area is under video surveillance.

Images may be recorded and/or monitored.

Information collected by the use of video equipment in this area is collected under the authority of the Municipal Act, 2001 in accordance with the provisions of the Municipal Freedom of Information and Protection of Privacy Act.

Any questions about this collection can be obtained by contacting City Clerk's Office at 519-740-4680 ext 4583”

Requests for disclosure

The City of Cambridge does not disclose a video record to any individual or organization except as permitted through MFIPPA.

1. Public requests for disclosure - Any person may make a written request for access to video records created through a video surveillance system through the freedom of information process. Access may depend on whether there is a justified invasion of another individual's privacy and whether any exempt information can be reasonably severed from the record. (through appropriate request form)
2. Internal requests for disclosure – City employees or consultants may request a copy of a video recording if it is necessary for the performance of their duties in the discharge of the corporation's function.
3. Law enforcement requests - The City may disclose a copy of a video recording to a law enforcement agency where there are reasonable grounds to believe that an unlawful activity has occurred and has been captured by the video surveillance system in accordance with section 32. (g) of MFIPPA.(through appropriate request form)

If video containing personal information is improperly disclosed or is suspected to have been disclosed to an unauthorized person, the employee or service provider who is aware of the disclosure must immediately inform the Freedom of Information Coordinator.

Live viewing

Live viewing is restricted to time periods when there is higher likelihood of safety and security concerns, or the commission of unauthorized activity in the area under surveillance. Live feed monitors are turned off when not in use. Viewing rights and responsibilities are outlined in Schedule B to this policy.

Retention and destruction

Video that has not been requested by the public, City employees or law enforcement agencies within the maximum retention period is considered transitory and is automatically erased by being overwritten.

RESPONSIBILITY

The City Clerk and delegated employees will:

- Respond to requests for disclosure under the freedom of information or applicable routine disclosure procedures;
- Ensure a public notice for video surveillance has been placed at all locations that have a video surveillance system;
- Respond to requests from the public and employees about the collection, use, and disclosure of personal information captured by a video surveillance system;

- Respond to appeals and privacy complaints received through the Office of the Information and Privacy Commissioner of Ontario (IPC);

The Director of Economic Development, the Corporate Property Manager, and the Manager of Technology and Support Services will:

- Ensure the appropriate use of the video surveillance system at the location is in compliance with this policy;
- Delegate and assign responsibility regarding who will act on their behalf in following procedures relating to this policy in their absence;
- Refer any requests for copies of surveillance video to the City Clerk or delegated employees;
- Investigate and report any privacy breaches to the City Clerk or delegated employees;
- Ensure that employees are monitoring compliance with the retention periods applicable to the video surveillance systems.

POLICY COMMUNICATION

These policies have been communicated through City Departments and Staff via meetings and written correspondence with the:

- Corporate Facility Manager
- Manager of Technology Services Support
- Assistant City Solicitor
- Deputy Clerk (Freedom of Information Officer)
- Manager of Transportation Engineering

External consultation includes:

- Downtown Cambridge BIA
- Regional Municipality of Waterloo (Legal Services and Engineering)
- Office of the Information and Privacy Commissioner of Ontario (IPC)
- Various private property owners

RELATED PROCEDURES

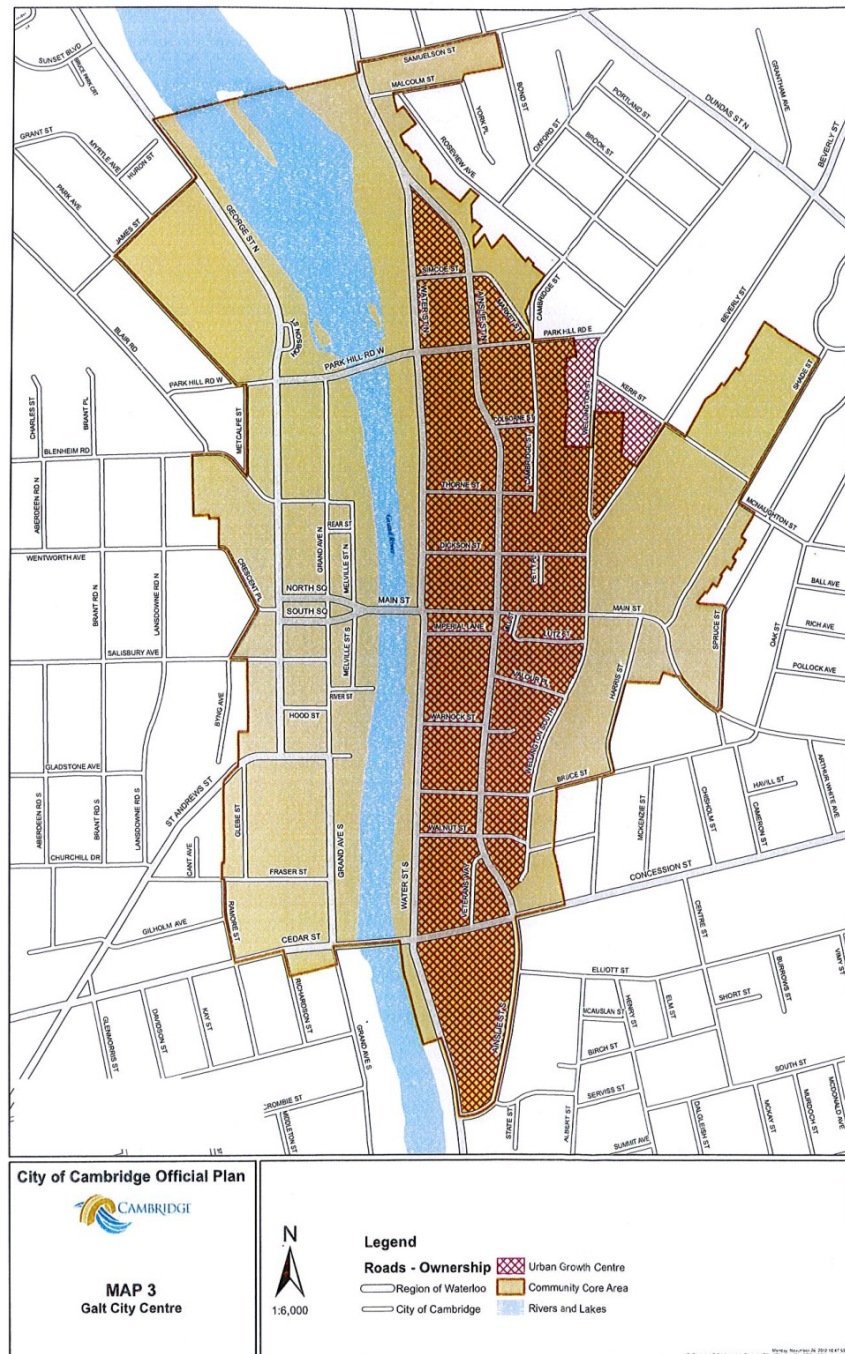
Please see 'Schedule B – Control Document' attached to the policy.

RELATED DOCUMENTS/LEGISLATION

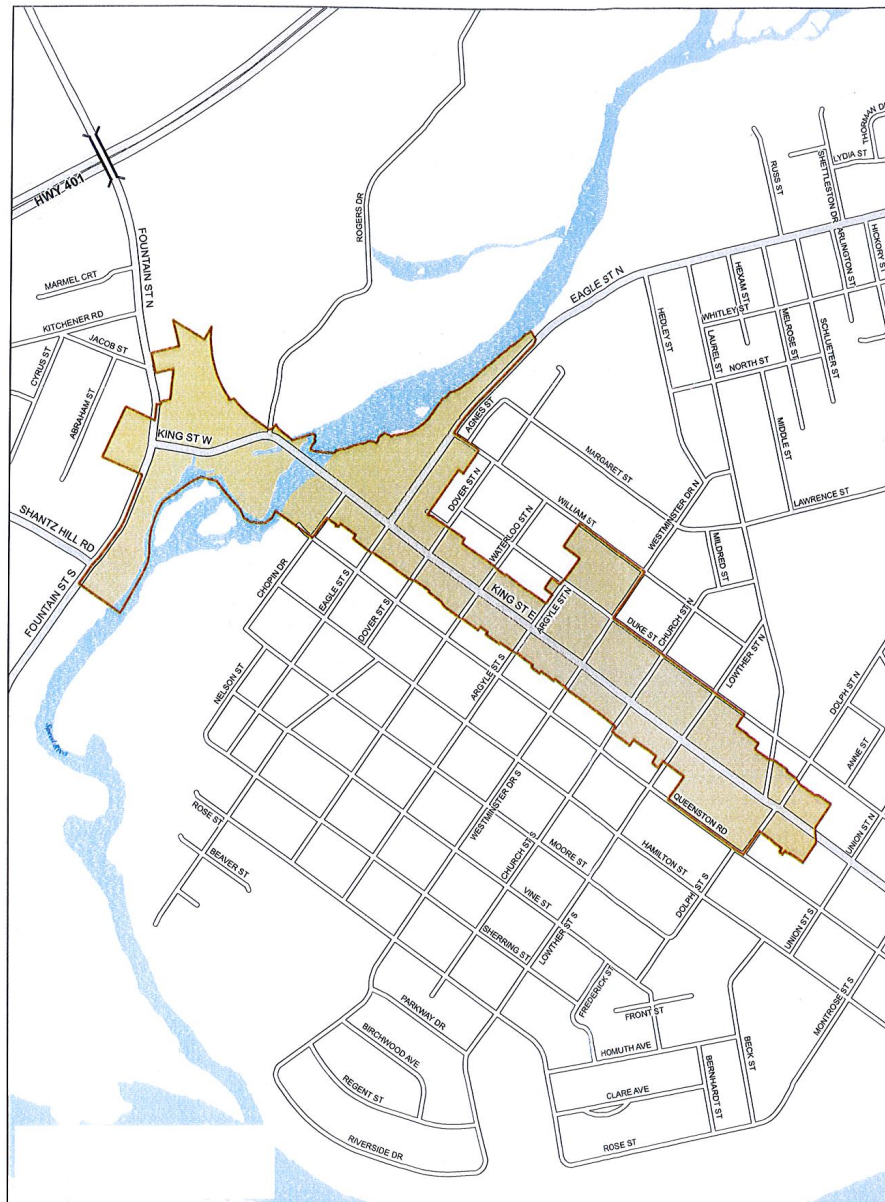
Municipal Freedom of Information and Protection Privacy Act

Information and Privacy Commissioner

Schedule 'A' Core Area Maps (Galt City Centre – as per Official Plan)



Schedule 'A' **Core Area Maps** **(Preston Towne Centre – as per Official Plan)**



City of Cambridge Official Plan



MAP 4
Preston Towne Centre



Legend

Roads - Ownership

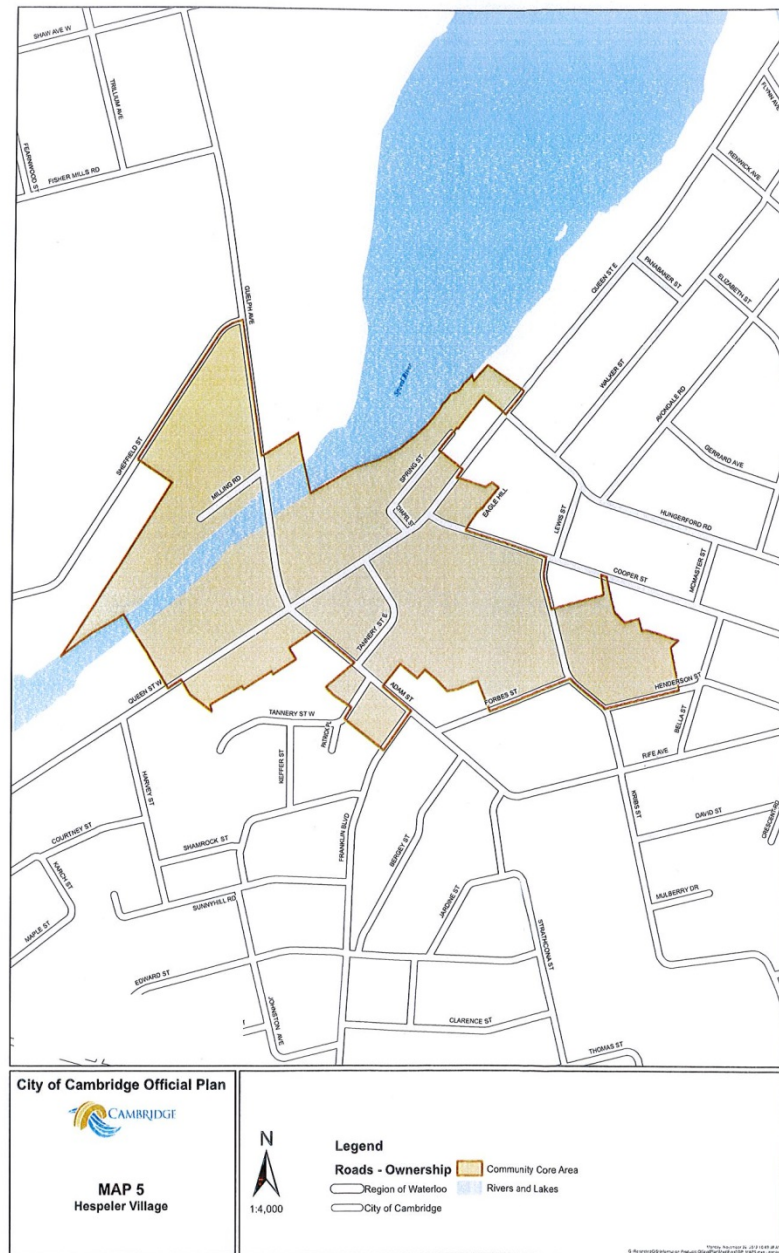
Province of Ontario or Region of Waterloo
 City of Cambridge

Community Core Area

Bridge

Rivers and Lakes

Schedule 'A' **Core Area Maps** **(Hespeler Village – as per Official Plan)**



Schedule 'B'

Control Document

1.0 Introduction

- 1.1 The City of Cambridge has adopted a policy related to the use of video surveillance systems within public areas in the Cambridge Core Areas. Those policies require that whenever the installation of video surveillance equipment is being considered within the City of Cambridge's Core Areas (as defined by the Cambridge Official Plan) the Director of Economic Development (or designate) will prepare, in conjunction with the City's Freedom of Information Coordinator, a comprehensive written control document for the operation of that particular system. This document is the required control document for the installation in the City of Cambridge Core Areas as defined by the Cambridge Official Plan.
- 1.2 A record of any adjustments made to the original system installation will be attached to this document as an amendment or a new version of the document may be created to reflect significant changes. Copies of this document and any amendments will be stored with the City Clerk or the Freedom of Information Coordinator.
- 1.3 Since images of individuals collected by this video surveillance system are considered to be the personal information of the individuals photographed the recordings are subject to the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).
- 1.4 The video system is to be installed to enhance safety and security of business owners, property owners, and the visiting public.

2.0 Notice of Collection

- 2.1 A written notice, in easily readable lettering, will be posted in the public area in a position easily viewed by the public. The notice will explain that the area is monitored by video cameras, why the cameras are in place and where members of the public can obtain further information about the installation. The sign should read: "To promote safety this area is under video surveillance. Images may be recorded and/or monitored. Information collected by the use of video equipment in this area is collected under the authority of the Municipal Act, 2001 in accordance with the provisions of the Municipal Freedom of Information and

Protection of Privacy Act. Any questions about this collection can be obtained by contacting City Clerk's Office at 519-740-4680 ext 4583.

3.0 Cameras

- 3.1 The cameras of the video surveillance system are currently installed as per Schedule B. Cameras will record activity in the public areas for 24 hours a day, 7 days a week. Locations are shown in the attached Location Map(s) at the end of this document. All the cameras are stationary and are pointed at public areas for monitoring and safety.
- 3.2 Locations of cameras are numbered and listed as per Schedule B.
- 3.3 None of the cameras described in Schedule B will be moved from the original locations nor will the views of the cameras be adjusted other than for normal panning, tilting and security required zoom adjustments without a review of the persons responsible for the initial installation. Only the Director of Economic Development (or designate) in coordination with the City Clerk and the Manager of Technology and Support Services and the Corporate Property Manager, may install, change or authorize a service provider or employee to install or change a camera's permanent setting.

4.0 Monitors

- 4.1 One secure monitor is located in the Office of the Corporate Property Manager. The monitor can only be viewed by the Director of Economic Development (or designate), the Manager of Technology and Support Services, and the Corporate Property Manager. Views on screens are not available to the general public.
- 4.2 The pan/swivel/tilt cameras may also be controlled using a web-based application through password-controlled access by the Manager of Technology and Support Services or by other Technology Services staff designated by the Manager of Technology Services with the permission of the Director of Economic Development (or designate), and the Corporate Property Manager.

5.0 Recording

- 5.1 Images are recorded on digital video servers with a storage area network (SAN) located in the server room. Recordings are retained for one month (30 days) or until storage capacity is reached. The data is then overwritten.

5.2 As noted above, there is no live monitoring of the system. Access by Technology Services staff is limited to ensuring the system functions according to specifications. The Manager of Technology and Support Services may view the recordings at the request of the Director of Economic Development (or designate) as needed for support purposes.

5.3 Recordings may be retained for a longer period of time for the purposes of insurance, liability, law enforcement or other similar issues (please note section 6.2 below).

6.0 Storage of and Access to Recordings

6.1 The recording and storage equipment will be stored in a secure, non-public area at all times.

6.2 In cases where the surveillance system records activities that relate to an insurance, liability, law enforcement or other similar issue, the appropriate section of the recording will be copied to suitable media and stored in a separate secure location for a period of no less than one (1) year or a longer appropriate length of time.

6.3 Access to the recordings will be restricted to the Director of Economic Development (or designate), the Manager of Technology and Support Services, the Freedom of Information Co-ordinator or designate, and the Corporate Property Manager.

6.4 The Freedom of Information Co-ordinator (or designate) is permitted to release copies of the records to a law enforcement agency in response to a verbal request only in situations involving an emergency, imminent danger or hot pursuit. All other requests for access by law enforcement authorities must be documented through the access request documentation utilized routinely by the Freedom of Information Co-ordinator.

6.5 Viewing of the recorded information is restricted to Director of Economic Development (or designate), the Manager of Technology and Support Services the MFIPPA Head/Freedom of Information Co-ordinator, or their designate, and the Corporate Property Manager. Viewing will be permitted only for purposes compatible with the original purpose for the installation of the surveillance system. Approved viewing of the recorded information must be conducted in private and in the presence of authorized persons only.

- 6.6 The Corporate Property Manager is the designated contact person for general inquiries regarding the operation of the surveillance cameras. The Freedom of Information Co-ordinator is the designated contact person for inquiries regarding the recordings.

7.0 Logs

- 7.1 A log will be kept to record access to the recordings. An entry will be made each time the recordings are consulted or any time a copy is made of any part of them. The log entry will note the person(s) accessing the recordings and the reason for access. The recording access log will be located in the Office of the Corporate Property Manager.
- 7.2 Recordings must be released if they are subject to a subpoena, search warrant, summons or other order of the courts or a quasi-judicial tribunal. In these cases a digital copy of the original recording will be provided. If the requesting parties require the hard drive a copy of the recording will be made before release of the hard drive. All actions taken in response to a subpoena etc. including the information that a copy was made will be entered into the log. A copy of the log entry will be filed with this document.

8.0 MFIPPA

- 8.1 Subject to paragraph 6.4, because the recordings are a “record” as defined in MFIPPA they may be requested by any person. All requests for access to recordings must be made through a written MFIPPA request. All MFIPPA requests must be forwarded to the City’s Freedom of Information Co-ordinator and will be considered on their merits and the requirements of MFIPPA.
- 8.2 Employees and service providers are subject to the provisions of MFIPPA in performing their functions related to the operation of video surveillance systems.

9.0 Notice of Collection Regarding the Use of Video Surveillance Systems

- 9.1 A Notice of Collection, required under section 29 of MFIPPA, will also be available to the public (see below 9.2). The Notice of Collection may be made available through the City website, public directories, or alternate formats such as pamphlets or signage based on the nature of the public’s use of specific facilities. The Notice may be revised on a site by site basis to reflect unique or specific uses of the images.

- 9.2 Notice of Collection - The collection of personal information by video surveillance systems is authorized under the Municipal Act. Surveillance systems will be used to ensure the safety of the residents and visitors; deter unsafe activities; deter loitering on municipal streets and around public buildings; and contribute to the Cambridge Core Area revitalization. Access to system equipment and recorded images is restricted to authorized staff. Surveillance images may be disclosed to law enforcement or other public agencies to assist in authorized investigations. Any questions about this collection can be obtained by contacting City of Cambridge clerk's office at 519-740-4680 extension 4583.

10.0 Signs

- 10.1 Notification signs will be placed in all viewing areas where the cameras are present. Signs will be visible to the public.

Sign Design:



Galt City Centre

1. Main Street at Water Street (intersection)
2. Dickson Street Parking Lot (Lot G5)
3. Main Street at Ainslie Street (intersection)
4. Main Street at Wellington Street (intersection)
5. Water Street Lot #2 (Lot G12 West pole)
6. Water Street Lot #2 (Lot G12 West pole)
7. Mill Street Lot (Lot G11 West pole)
8. Main Street Lot (Lot G10 West pole)
9. Mill Street Lot (Lot G11 East pole)
10. Water Street (Pedestrian Bridge)

Phase 2

11. Water Street (Pedestrian Bridge)
12. Dan Spring Way Trail
13. Dan Spring Way Trail
14. Dan Spring Way Trail
15. Dan Spring Way Trail
16. Dan Spring Way Trail



POLICY TITLE	Use of Corporate Cameras Policy
CATEGORY	Choose an item.
POLICY NUMBER	Leave Blank – Clerk’s team will input once finalized/approved
DEPARTMENT	Corporate Services
POLICY AUTHOR	City Clerk
POLICY TYPE	Administrative Policy
APPROVED BY	Choose an item.
EFFECTIVE DATE	(10/19/2021) Insert date policy is effective
REVIEW DATE	(10/19/2023) Insert date policy is to be reviewed

POLICY STATEMENT

The City of Cambridge (the Municipality) recognizes the need to balance an individual’s right to privacy and the need for the safety and security of its residents, visitors, municipal employees and property while integrating best practices with a responsible use of technology to minimize privacy intrusions.

PURPOSE

The object of this policy is to govern the Use of Corporate Cameras within the City of Cambridge to enhance the safety and security to prevent unauthorized activities and reduce risk and liability exposures.

DEFINITIONS

City: The Corporation of the City of Cambridge.

Clerk: The City Clerk of the Corporation of the City of Cambridge.

Consistent purpose: Personal information collected by the City of Cambridge used for the purpose for which it was collected.

City business: The individual to whom the information relates might reasonably expect the use/disclosure of their personal information for those consistent purposes.

Control (of a record): The power or authority to make a decision regarding the use or disclosure of a record.

Custody (of a record): The keeping, care, watch, preservation or security of a record for a legitimate business purpose. While physical possession of a record may not always constitute custody, it is the best evidence of custody.

Destruction: The physical or electronic disposal of records or data by means of disposing, recycling, deletion, or overwriting. This also includes the destruction of records or data residing on computers and electronic devices supplied or paid for by the Corporation.

Freedom of information process: A formal request for access to records made under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Head: The City Clerk designated as head for the administration of the Municipal Freedom of Information and Protection of Privacy Act.

Information and Privacy Commissioner: The Information and Privacy Commissioner of Ontario (commonly referred to as the IPC).

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA): Is the legislation that governs access, use, and disclosure of information held by the Municipality.

AUTHORITY

The IPC provides oversight to Ontario's access and privacy laws and the administration of how institutions may collect, use and disclose personal information. The IPC provides the public with the right of access to government-held information while ensuring that personal information remains private and secure.

In addition to overseeing the province's access and privacy laws, the IPC also serves both the government and public to:

- resolve appeals when access to information is refused;
- investigate privacy complaints related to personal information;
- ensure compliance with the acts;
- review privacy policies and information management practices;
- conduct research on access and privacy issues and provide comment on proposed government legislation and programs;
- educate the public, media and other stakeholders about Ontario's access and privacy laws and current issues affecting access and privacy.

The Commissioner is an officer of the Legislature who is appointed by, and reports to, the Legislative Assembly of Ontario.

This policy has been developed in accordance with the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and has been drafted to conform with the practices outlined by the IPC Guidelines for the Use of Video Surveillance.

As detailed in Section 28(2) of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), personal information may be collected without consent when it is:

1. Expressly authorized by statute or by-law,
2. Used for the purpose of law enforcement, or
3. Necessary to the proper administration of a lawfully authorized activity.

SCOPE

This policy applies to the use of all camera systems within the City of Cambridge.

To all City of Cambridge employees, including full-time, part-time, causal, contract, volunteer, and co-op placement employees, as well as contractor and service providers while performing authorized activities for the City.

And does not apply to covert use used as an investigation tool for law enforcement purposes or in contemplation of litigation.

The guidelines outline are not intended to apply to workplace surveillance systems installed by an institution to conduct surveillance of employees.

POLICY

The City of Cambridge is required to comply with Ontario's privacy laws and therefore has an obligation with respect to the notice, collection, access and use, disclosure, retention and disposal of personal information, including fundamental data minimization principles

While the use of camera systems are installed for safety and security reasons, the use of camera systems must minimize privacy intrusion.

Guideline to Follow to the Installation of Camera Systems

Prior to the installation of camera systems, the following factors much be considered:

- the use of camera systems should be justified on the basis of verifiable, specific reports of incidents of crime, or significant safety concern;

- a privacy impact assessment must be conducted on the effects that the proposed camera system may have on personal privacy, and the ways in which any adverse effect can be mitigated;
- the proposed design and operation of the camera system should minimize intrusion;
- whether or not additional sensory information, such as sound, needs to be captured.

When designing a camera system and installing equipment the following must be considered:

- the camera system may operate at any time in a 24-hour period;
- the camera system should be installed to only monitor those spaces that have been identified as requiring camera use;
- the ability to adjust cameras should be restricted, if possible, so that the cameras do not record and operators cannot adjust or manipulate cameras to overlook spaces that are not intended to be covered by the camera use program, such as windows in adjacent buildings or onto adjacent properties;
- equipment should never monitor the inside of areas where the public or employees have a higher expectation of privacy (e.g. change rooms and washrooms);
- where possible, camera use should be restricted to periods where there is a demonstrably higher likelihood of crime being committed and detected in the area under camera use;
- viewing and recording equipment must be located in a strictly controlled area;
- only authorized and trained staff shall have access to the controlled access area and that reception/recording equipment;
- every reasonable attempt should be made to ensure camera monitors are not in a position that enables the public and/or unauthorized staff to view the monitors.

Use of Recorded Information:

The information collected through camera recordings shall only be used for the purposes of:

- enhancing the safety and security of employees, the public, and corporate assets;
- preventing unauthorized activities upon or involving City property;
- assisting in investigating unlawful activity;
- assessing the effectiveness of safety and security measures;
- investigating an incident involving the safety or security of people, facilities or assets;
- providing evidence as required to protect the City's legal rights;
- investigating an incident or allegation of serious employee misconduct;
- investigation and incident involving a potential or active insurable claim; or
- a consistent purpose.

Notice of Use of Camera Systems

In order to provide notice to individuals that cameras are in use:

- the municipality shall post signs, visible to members of the public, at all entrances and/or prominently displayed on the perimeter of the grounds under camera use; (Appendix A);
- the notification requirements of this sign must inform individuals, using words and symbols, of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used; and the title, business address, and telephone number of someone who can answer questions about the collection;
- A map of all authorized camera locations will be available on the Municipal website.

Personnel Authorized to Operate Camera Equipment

- Only the City Clerk, or personnel authorized by the City Clerk, shall be permitted to operate camera use systems.

Equipment/Types of Recording Devices

The Municipality may use Digital Camera Recorders (DVR) in its camera systems. Facilities using camera recorders will retain these records for a period of up to 30 days, depending on the recording device and technology. A record of an incident will only be stored longer than 30 days where it may be required as part of a criminal, safety, or security investigation or for evidentiary purposes. Monitors will be kept in a secure location where they are not visible to the public.

Record Identification

All records (storage devices) shall be clearly identified (labeled) as to the date and location of origin. They shall be labeled with a unique, sequential number or other verifiable symbol. In facilities with a DVR that stores information directly on a hard drive, the computer time and date stamp shall be understood to be this identification. In facilities with a VCR or other recording mechanism using a removable/portable storage device, the operator shall affix a label to each storage device identifying this information.

Access Logs

Access to cameras will be monitored with a record of all activities related to camera devices recorded in an access log. Access Logs will include all information regarding the use, maintenance, and storage of records and all instances of access to, and use of, recorded material. All access log entries will also detail authorized staff, date, time, and activity. Access logs must remain secure with only the City Clerk authorized to review or remove access logs from the secure location.

Access to Records

Access to camera records shall be restricted to authorized personnel only in order to comply with their roles and responsibilities as outlined in the Camera Use Policy. Any staff accessing records should sign a written agreement to adhere to this policy, including an undertaking of confidentiality.

Storage

All storage devices that are not in use must be stored securely in a locked receptacle located in an access-controlled area.

Access Requests: Public Process

With exception of requests by law enforcement agencies, all requests for camera records should be directed to City Clerk's office for processing. A person requesting access to a record should make a request in writing either in the form of a letter or the prescribed

Access/Correction Request Form (Appendix B) and submit it to the City Clerk under MFIPPA.

The individual requesting the record must:

- Provide sufficient detail (the approximate time and date, the location - if known - of the incident, etc.) to enable an experienced employee, upon a reasonable effort, to identify the record; and,
- At the time of making the request, pay the prescribed fees as provided for under the Act.

Access Requests: Law Enforcement

If access to a camera Use record is required for the purpose of a law enforcement investigation, the requesting Officer must complete the Law Enforcement Officer Request Form (Appendix C) and forward this form to the City Clerk. While there may be other situations where the disclosure of camera use footage is permitted, camera footage may be disclosed to a law enforcement agency when:

- the law enforcement agency approaches the Municipality with a warrant requiring the disclosure of the footage, as per section 32(e) of MFIPPA;
- the law enforcement agency approaches the Municipality, without a warrant, and requests the disclosure of footage to aid an investigation from which a proceeding is likely to result, as per section 32(g) of MFIPPA;
- staff observe an illegal activity on municipal property and disclose the footage to a law enforcement agency to aid an investigation from which a proceeding is likely to result, as per section 32(g) of MFIPPA;
- staff will provide the recording for the specified date and time of the incident as requested by the Law Enforcement Officer and record the following information in the facility's camera logbook:
 - i) the date and time of the incident including the designated name/number of the applicable cameras;
 - ii) the time and date the copy of the original record was sealed;
 - iii) the time and date the sealed record was provided to the requesting Officer;
 - iv) the case file number of the agency's investigation;
 - v) a description of the circumstances justifying the disclosure;

- vi) the amount of footage involved;
 - vii) the name, title and agency to whom the footage is being disclosed;
 - viii) the legal authority for the disclosure;
 - ix) the means used to disclose the footage; and
 - x) if the record will be returned or destroyed after use by the Law Enforcement Agency.
- this must only be completed by an individual(s) authorized in a private, controlled area that is not accessible to other staff and/or visitors;
 - in order to protect privacy, the Municipality will, whenever possible, strongly encrypt camera footage at rest and when transmitted across open, public networks, and store physical records of footage, such as discs, memory cards or servers, in a locked facility.

Custody, Control, Retention and Disposal of Records

The Municipality retains custody and control of all original camera records not provided to law enforcement.

Camera records are subject to the access and privacy requirements of the MFIPPA, which includes but is not limited to the prohibition of all staff from access or use of information from the camera system, its components, files, or database for personal reasons.

With the exception of records retained for criminal, safety, or security investigations or evidentiary purposes, or as otherwise required by law, the Municipality must not maintain a copy of recordings for longer than 30 days.

Any records that are accessed or disclosed will be retained for one year, as per Regulation 823 of MFIPPA.

The Municipality will make all reasonable efforts to ensure the security of records in its custody or control and ensure their safe and secure disposal.

Old storage devices must be disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased prior to disposal, and cannot be retrieved or reconstructed. Disposal methods may include shredding, burning, or erasing, depending on the type of storage device.

Unauthorized Access and/or Disclosure (Privacy Breach)

Staff who become aware of any unauthorized disclosure of a camera record in contravention of this Policy and/or a potential privacy breach are to immediately notify the City Clerk. After this unauthorized disclosure or potential privacy breach is reported:

- Upon confirmation of the existence of a privacy breach, the City Clerk shall notify the Information and Privacy Officer of Ontario (IPO) and work constructively with the IPO staff to mitigate the extent of the privacy breach and to review the adequacy of privacy protection with the existing policy.
- Staff shall inform the City Clerk of events that have led up to the privacy breach.
- Staff shall work with the City Clerk to take all reasonable actions to recover the record and limit the record's disclosure.
- The City Clerk shall notify affected parties whose personal information was inappropriately disclosed.
- The City Clerk shall investigate the cause of the disclosure with the goal of eliminating potential future occurrences.

Intentional wrongful disclosure or disclosure caused by negligence by employees may result in disciplinary action up to, and including, dismissal. Intentional wrongful disclosure or disclosure caused by negligence by service providers (contractors) may result in termination of their contract.

Awareness and Training for Municipal Employees

Authorized staff that have access to or are required to view footage will be required to attend mandatory awareness training on the use of camera systems.

Inquiries from the Public Related to the Camera Use Policy

A staff member receiving an inquiry from the public regarding the Camera Use Policy shall direct the inquiry to the City Clerk.

Review of Camera Use Policy

This policy shall be reviewed every 2 (two) years by the City Clerk who will forward recommendations for update, if any, to Council for approval.

POLICY COMMUNICATION

This policy will be available on the City of Cambridge's Policy and Procedure SharePoint page.

RELATED PROCEDURES

“There are no related procedures.”

RELATED DOCUMENTS/LEGISLATION

The Municipal Freedom of Information and Protection of Privacy Act. R.S.O. 1990, c. M.56

Ontario Regulation 823 under the Municipal Freedom of Information and Protection of Privacy Act

FIPPA and MFIPPA – Bill 8 – Recordkeeping Amendments

REFERENCE MATERIAL

IPC: Guidelines for the Use of Video Surveillance

https://www.ipc.on.ca/wp-content/uploads/Resources/2015_Guidelines_Surveillance.pdf

Appendix A

**To promote safety this
area is under video
surveillance**

Images may be recorded and/or monitored



Information collected by the use of video equipment in this area is collected under the authority of the Municipal Act, 2001 in accordance with the provisions of the Municipal Freedom of Information and Protection of Privacy Act.

Any questions about this collection can be obtained by contacting City Clerk's Office at 519-740-4680 ext 4583



Appendix B



Access/Correction Request
Freedom of Information and Protection of Privacy
 A \$5.00 application fee is required for ALL requests made under the
Municipal Freedom of Information and Protection of Privacy Act.
 Cheque or money orders should be made payable to the City of Cambridge.

Request for: <input type="checkbox"/> General Records <input type="checkbox"/> Access to Own Personal Information <input type="checkbox"/> Correction to Own Personal Information	Name of Institution request made to: <div style="text-align: center; font-size: 1.2em; font-weight: bold;">CITY OF CAMBRIDGE</div>
--	--

If request is for access to or correction of your own personal information records please indicate last name appearing on records <input type="checkbox"/> Same as below, or: _____		
Last Name:	First Name:	
Mailing Address:		
City / Town:	Province:	Postal Code:
Phone Numbers: (Day): _____ (Mobile): _____		
Email Address: _____		

** Please note that the use of personal contact information will only be used as a communication tool related to this request.
 Records packages will ONLY be available via Regular Mail or for Pick Up.

Please provide a detailed description of requested records, personal information records or personal information to be corrected. (If you are requesting access to, or correction of your personal information, please identify the personal information bank or record containing the personal information, if known). (Please use the back of this form if additional space is required). <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div>
Note: If you are requesting a correction of personal information, please indicate the desired correction and, if appropriate, attach any supporting documentation. You will be notified if the correction is not made and you may require that a statement of disagreement be attached to your personal information.

Preferred method of access:	<input type="checkbox"/> Examine Original <input type="checkbox"/> Receive Copy	Signature: _____	Date: _____
------------------------------------	--	-------------------------	--------------------

Personal information contained on this form is collected pursuant to Municipal Freedom of Information and Protection of Privacy legislation and will be used for the purpose of responding to your request. Questions about this collection should be directed to the City Clerk's Office of the Corporate Services Department @ 519-740-4680.

For Institution Use Only:		
Date Received:	Request Number:	Response Date:

Appendix C



LAW ENFORCEMENT OFFICER REQUEST FORM DISCLOSURE OF PERSONAL INFORMATION

Corporate Services Department – Office of the City Clerk

The following information is being requested under section 32(g) of the Municipal Freedom of Information and Protection of Privacy Act (the Act) which provides for the disclosure of records containing personal information of an individual for the purpose of aiding an investigation with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

PART ONE: DETAILS OF REQUEST (To be completed by Law Enforcement Officer):				
Incident Date:		Incident Location:		Incident Time:
Information Requested (please describe):				
Occurrence Reference No.:		Review Original Documents:		Copies Requested:
		YES	NO	YES NO
Name of Law Enforcement Agency:		Name of Law Enforcement Officer:		Badge / ID No.: Telephone:
Signature of Law Enforcement Officer:		Date of Request:		
PART TWO: INFORMATION/RECORD(S) DISCLOSED (To be completed by City Staff disclosing information/records):				
Department / Division:				
Information / Record(s) / File(s) Disclosed (please describe):				
Disclosure of Information by City Staff:				
Name of Staff Member:		Title / Position:		Telephone:
Signature of Staff Member:				Date: