Transportation Management Centre
Traffic Monitoring Camera Protocol

Authority for protocol: Chief Administrative Officer
Last updated: 19-Apr-2021

Introduction:	The City of Winnipeg's Public Works Department (PWD) uses a traffic management system, enabled with real-time data from Pan/Tilt/Zoom (PTZ) cameras, to ensure streamline City traffic flow. PWD recognizes the need to balance the collection of traffic data with an individual's right to privacy. The system configurations and administrative controls through this protocol follow Privacy by Design principles and aligns with the City's obligations under the *Freedom of Information and Protection of Privacy Act*.
Program Title:	Transportation Management Centre (TMC) - Traffic Monitoring Cameras
Program Purpose:	Collect real-time and recorded information about the flow of traffic, including traffic incidents, and use that information to effectively manage City traffic flow.
Parties Involved:	City of Winnipeg and 3rd party Video Management System
Contact Person:	TMC Supervisor

DEFINITIONS

Incident	An event or occurrence that causes, or has the potential to cause, traffic congestion, traffic disruption or damage to City property.
Traffic	Any vehicle, cycle, and pedestrian movement.
TMC cameras	Pan/Tilt/Zoom (PTZ) cameras installed at traffic signals throughout the City of Winnipeg where real-time traffic data is needed for the TMC to carry out the program's purpose.
TMC video	Recorded information captured by the TMC cameras.
TMC visual clip	Portion of a TMC video that captures a specific incident and/or time frame and is stored as a distinct file from the original TMC video.

GENERAL INFORMATION

Governance

1 TMC cameras are a tool for monitoring traffic flow and traffic related incidents; specifically, for

(a) Managing and confirming reports of traffic related incidents.
(b) Detection of damage to City of Winnipeg property.
(c) Incident investigations (i.e., TMC's Collision Review Program).
(d) Research and analysis of City of Winnipeg traffic flow.

2 Operation of TMC cameras or use of TMC video is limited to authorized purposes.

(a) TMC cameras shall not be operated by any employees for the sole purpose of satisfying anyone's personal interest in any individual.

(b) TMC cameras shall not be used by employers to monitor employee locations or performance.

3 The TMC cameras, related equipment, and any recorded images subsequently generated by recording equipment are the property of and under control of the City of Winnipeg. The third-party video management software company must not have access to any information recorded by TMC cameras.

4 The collection of, access to, the production of, and/or maintenance of records created in the operation of TMC cameras shall be in accordance with this protocol and:

(a) The Freedom of Information and Protection of Privacy Act (FIPPA)

(b) Records Management By-Law 123/2020

(c) Administrative Standard AS-015 Access to Information and Protection of Privacy

(d) Administrative Standard IT-004 Individual Responsibility for IT Security

(e) TMC Social Media Guidelines

5 Use and disclosure of recorded information captured by TMC cameras must be managed in accordance with FIPPA, and according to this Protocol.

6 A copy of this protocol will be posted on City's Access and Privacy Office webpage and the Transportation Management Centre webpage.

Operations and Records

7 The Traffic Signals Branch is responsible for the Transportation Management Centre and the control, operation, and maintenance of the TMC cameras.

(a) The Transportation Management Centre operates Monday-Friday, 06:00-19:00, with closures on statutory holidays.

(b) TMC cameras operate 24 hours/day, 365 days/year.

8 TMC video and their associated third-party System User Access Logs is retained for up to 7 days. Information may be recorded over earlier, depending on TMC requirements and/or technological limitations.

9 TMC video used by the TMC's Collision Review Program will be retained for 5 years, with retention needs reviewed annually.

10 To provide notice to the public that video recording is in operation, the TMC will share information and a notification statement about the TMC cameras on the City website.

Privacy Statement

11 This privacy statement must be posted in the Transportation Management Centre section of the City of Winnipeg website to satisfy FIPPA's public notification requirements.

(a) If more effective mechanisms for public notification become available, they must be explored as part of the regular protocol review process.

(b) The online list of fixed locations referred to in the privacy statement must be maintained for accuracy.

Privacy Statement

The purpose of the TMC traffic cameras is to monitor, address, and study traffic flows. TMC traffic cameras are operated at fixed locations on the roadways to maximize coverage.

Default camera settings do not allow for the capture of personally identifiable information, such as license plate numbers, or individual faces. Pan/Tilt/Zoom capabilities may be used when monitoring specific traffic congestion incidents, traffic disruptions, suspected damage to City of Winnipeg property, when a traffic study is being conducted, or when used for law enforcement or crime prevention. Any personally identifiable information collected by cameras during Pan/Tilt/Zoom operation, is done pursuant to section 36(1)(b) or 36(1)(c) of *The Freedom of Information and Protection of Privacy Act* (FIPPA), depending on the activity. Through camera placement and remediation measures (such as privacy masks), TMC traffic cameras are not set to view locations where an individual has a reasonable expectation of privacy.

TMC traffic cameras do not operate as a surveillance tool, however, where approved under exceptional circumstances, TMC cameras may be used by Winnipeg Police Service for law enforcement or crime prevention purposes, as permitted under FIPPA, section 36(1)(c).

Video from TMC traffic cameras is retained for up to 7 days after which it is overwritten. Copies of TMC traffic video may be requested under Part 2 of FIPPA through City Clerk's within 7 days of the incident, since it is overwritten after that point.

If you have any questions regarding this collection or use of this information, please contact the Corporate Access and Privacy Officer by mail to City Clerk's Department, Administration Building, 510 Main Street, Winnipeg MB, R3B 1B9, or by telephone at 311.

Audit

12 The PWD Records and Information Management Coordinator must undertake an annual audit of the TMC Traffic Monitoring PTZ Cameras Program to evaluate compliance with relevant policies, procedures, and legislation to ensure that videos are accessed and used for their intended purposes, that security safeguards are followed and are adequate, and to identify any unintended negative impacts.

13 The portion of the audit related to law enforcement requests for access to TMC video and/or camera control will be led by the Corporate Access and Privacy Officer with the collaboration of the PWD Records and Information Management Coordinator and a member of the WPS Legal Counsel Unit.

ROLES AND RESPONSIBILITIES

14 **Chief Administrative Officer** shall

- Review and approve updates to this protocol.
- Ensure that PWD and WPS adhere to policies and protocols governing use of TMC Cameras.
- Receive and assess requests from the WPS Chief for temporary re-tasking of TMC cameras for law enforcement or crime prevention.
- Consult, as needed, on access and privacy matters with the Corporate Access and Privacy Coordinator.
- Communicate relevant decisions to the WPS Chief, Director of Public Works, and Corporate Access and Privacy Officer.

15 **Director, Public Works** shall

- Ensure compliance with this protocol.
- Communicate relevant TMC operational issues or service delivery concerns to the CAO.

- Communicate relevant decisions to the Engineer Traffic Signals, TMC Supervisor, and PWD Records and Information Management Coordinator.
- Ensure clear communication of and adherence to this protocol and related procedures by TMC supervisors and by all employees within their area of control.
- Ensure that all relevant employees receive training on their obligations under the Freedom of Information and Protection of Privacy Act, as recommended by the Corporate Access and Privacy Officer.
- Provide immediate mediation for contravention of this protocol.

16 **Engineer, Traffic Signals** shall

- Manage TMC as a part of the Traffic Signals Branch.
- Communicate relevant TMC operational issues or service delivery concerns to the Director, Public Works.
- Communicate relevant decisions to the TMC Supervisor and PWD Records and Information Management Coordinator.
- Support TMC operations and, if needed, assist with resolution of issues.

17 **TMC Supervisor** shall

- Supervise day-to-day operations of the Traffic Monitoring Camera Program.
- Maintain a log of all access, maintenance, and repairs to third-party software.
- Delegate various responsibilities under this protocol to Designated Employees.
- Maintain a list of Designated Employees who are authorized to access the TMC Cameras and/or their recordings.
- Process requests from Designated Employees involving the creation, disclosure, destruction, erasure, or alteration of TMC records, in consultation with the PWD Records and Information Management Coordinator.
- Review camera locations and positioning to minimize impact to individual privacy rights and, as needed, employ appropriate remediation measures, such as privacy masks.
- Operationalize CAO decisions to authorize temporary re-tasking of TMC Cameras for WPS control, per direction provided in each circumstance.
- Administer requests for access to TMC video.
- Provide relevant information and records to the PWD Records and Information Management Coordinator for the program audit (yearly) and review this protocol (every two years).

18 **PWD Records and Information Management Coordinator** shall

- Conduct an annual audit of the Traffic Monitoring Camera Program, including third-party video management software, in cooperation and collaboration with the Corporate Access and Privacy Officer.
- Coordinate and respond to FIPPA requests for TMC video, as directed by the Access and Privacy Office.
- Administer internal camera and video requests, MPI requests, and external research requests, in consultation with the TMC Supervisor.
- Provide general advice and guidance in the interpretation and execution of this protocol as it relates to access to information, privacy, and records/information management.

19 **Designated Employees** (e.g., TMC Operators, Timing Engineers, Traffic Signals Branch Engineers, and Traffic Signals Branch First Responders) shall

- Read and sign TMC Cameras Confidentiality Form agreeing to abide by the terms in the form

- Use Traffic Monitoring Camera Program credentials provided by the TMC Supervisor, keep them in confidence, and ensure workstation maintains the updated third-party management software program.
- Follow this protocol and other related Administrative Standards/procedures when performing assigned duties.
- Refrain from accessing, using, or disclosing information contained in the TMC video for personal reasons, and refrain from creating, disclosing, destroying, erasing, or altering any record without written authorization from the TMC Supervisor.

20 **Corporate Access and Privacy Officer** shall

- Advise and support the CAO on access and privacy matters related to this protocol.
- Advise and support PWD and WPS employees on access and privacy matters related to this protocol.
- Consult and collaborate with a member of the WPS Legal Counsel Unit regarding WPS requests that do not comply with the protocol or on other WPS-related issues, as needed.
- Collaborate with the PWD Records and Information Management Coordinator on the annual audit of the Traffic Monitoring Camera Program and conduct the law enforcement request portion of the audit in consultation with a member of the WPS Legal Counsel Unit.

21 **WPS Authorized TMC Camera Users** shall

- Use temporarily re-tasked TMC Cameras per written approval of the CAO, abiding by WPS protocols and relevant legislation.

EQUIPMENT

TMC camera installations

Figure 1:
Type of camera used by TMC for traffic monitoring

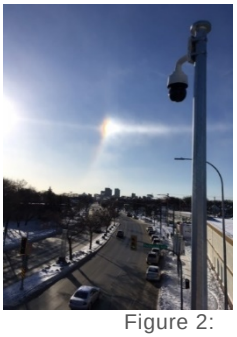

Figure 2:
Installed TMC camera

22 TMC camera video recording equipment is located at various locations in the right of way dependent on the City of Winnipeg's TMC's needs and coverage.

23 TMC cameras are operated at locations to maximize coverage of the road network. Cameras shall not be installed at locations where an individual has a reasonable expectation of privacy and remediation measures may be used to restrict zoom in view around areas where privacy is expected.

Security

24 All monitoring, operation and recording equipment associated with TMC cameras is located on City of Winnipeg Information Technology (IT) Servers located at 510 Main St. The server room is locked with access only to designated IT employees. Only employees designated by the TMC Supervisor shall have access to the TMC operating system or IT servers.

(a) Authorized Camera User Logs are maintained for one year, are reviewed regularly by the TMC Supervisor, and are included in the annual audit of the TMC Traffic Monitoring PTZ Cameras Program.

(b) Access to TMC camera recordings is restricted and limited to designated employees

(c) Workstations and software are accessed with unique log in IDs/Passwords

25 Access to TMC Cameras is limited to only what is needed to accomplish an authorized activity. Limitations may include the following measures: restriction to number of cameras available for access, restriction of camera ownership time/time the user has priority of control of a camera, restriction of pan/tilt/zoom (PTZ) capability, zero control of camera; and view only restriction.

REQUESTS FOR TMC CAMERA CONTROL

Law Enforcement Requests for TMC Camera Control

26 Under *The Freedom of Information and Protection of Privacy Act* and *The Charter of Rights and Freedoms*, individuals have privacy rights that ensure they can go about their lives without fear of government indiscriminately recording their activities or communications. However, there are times when a government's duty to enforce laws, or prevent crimes might outweigh individual privacy rights. Accordingly, in exceptional circumstances, the Winnipeg Police Service Chief (or delegate) may submit a written request to the CAO for the temporary re-tasking of TMC cameras for a law enforcement or crime prevention purpose.

This process does not replace or impact existing processes for WPS to receive judicial authorization for surveillance, but can be relied on when other authorization processes are impracticable. In such circumstances, the collection of personal information through surveillance may be authorized under FIPPA s.36(1)(c).

(a) If a request for TMC Camera Control is received from an outside law enforcement organization, this process shall be followed, as practicable.

(b) If anyone other than the CAO receives a request for TMC Camera Control, the request is to be forwarded to the CAO immediately for decision-making.

27 The CAO must assess the proposed surveillance through consideration of the following questions, document the decision-making, and may wish to consult with the Corporate Access and Privacy Officer:

(a) What is the situation presented by WPS and why do they believe that the proposed surveillance is necessary for law enforcement or crime prevention?

(b) Did WPS request judicial authorization for the proposed surveillance. If yes, what was the response. If no, why not?

(c) Has WPS implemented, explored, and/or exhausted other measures that could meet their need in full or in part without infringing on the privacy rights of individuals?

(d) Is the scope (e.g., number/locations of cameras) and time frame for the proposed surveillance limited and reasonable for the stated purpose? For instance, TMC cameras along a protest route for 12 hours vs. all TMC cameras for three days.

(e) What are the operational impacts for the TMC if the requested cameras are re-tasked? For instance, a camera cannot be controlled simultaneously by multiple users so when a camera is re-tasked to WPS, it is unavailable for its mandated purpose such as traffic management for the area impacted by a protest.

(f) Does the situation and rationale presented by WPS outweigh the Charter-protected freedom of expression, freedom of political affiliation, and privacy rights of the individuals gathering??

(g) Is more public notice than the TMC's online privacy statement warranted for transparency and to deter criminal activity (e.g., event perimeter signage, TMC tweet notification of altered operations, notice in a City media release about all aspects of the event)?

(h) What is the potential impact of the proposed surveillance on the public's confidence or trust in the City and is consultation (internal or external to the City) warranted for a fulsome decision and/or community buy-in?

28 Video recorded by the TMC cameras is retained for up to 7 days. If WPS requires copies of the video created during the surveillance exercise, it must be requested from TMC within that period. Requested video must be transferred via the secure WPS site. WPS records management rules and retention periods apply to the video once they receive their copies.

29 WPS requests for TMC camera control and/or video are part of the Audit, unless it would harm a law enforcement purpose.

30 Under Part 2 of FIPPA, individuals may request access to their personal information within the custody or control of the City. Accordingly, any FIPPA requests from the public for videos transferred to WPS must be directed to the WPS FIPPA Office for response.

City Department Requests for TMC Camera Control

31 All internal requests for TMC camera control, other than Law Enforcement Requests or those mandated by the Traffic Monitoring Camera Program, must be submitted on the "Internal Request for TMC Traffic Monitoring Camera Control" form to the TMC Supervisor for assessment and decision-making in consultation with the Public Works Department (PWD) Records and Information Management Coordinator. Requests must be assessed to determine whether use of the requested camera use is authorized under FIPPA s.36(1) or whether use of the requested TMC visual clip is authorized under either FIPPA s.43(a) in conjunction with FIPPA s.45, or FIPPA s.43(c) in conjunction with an applicable portion of FIPPA s.44(1).

REQUESTS FOR TMC VIDEO/VISUAL CLIPS

Public Works by-law enforcement requests

32 Requests for TMC video/visual clips for by-law enforcement purposes must be submitted on "Law Enforcement Request for Personal Information" form to the TMC Supervisor for assessment and decision-making in consultation with the PWD Records and Information Management Coordinator. Requests must be assessed to determine whether use of the requested information is authorized under FIPPA s.43(c) in conjunction with FIPPA s.44(1)(r).

All other internal access requests

33 Internal requests to use TMC video/visual clips for any purpose, other than those mandated by the Traffic Monitoring Camera Program must be submitted on the "Internal Request for TMC Traffic Monitoring Camera Video" form to the TMC Supervisor for assessment and decision-making in consultation with the PWD Records and Information Management Coordinator. Requests must be assessed to determine whether use of the requested camera use is authorized under FIPPA s.36(1) or whether use of the requested TMC visual clip is authorized under either FIPPA s.43(a) in conjunction with FIPPA s.45, or FIPPA s.43(c) in conjunction with an applicable portion of FIPPA s.44(1).

MPI requests

34 Requests from MPI to use TMC video/visual clips must be submitted on the "MPI Request for TMC Traffic Monitoring Camera Video" form to the TMC Supervisor for assessment and decision-making in consultation with the PWD Records and Information Management Coordinator.

35 Requests must be assessed to determine whether disclosure of the requested TMC visual clip is authorized under FIPPA s.44(1)(e).

External research requests

36 Requests to use TMC Cameras or TMC video/visual clips for external research purposes must be submitted on the "External Research Request for TMC Traffic Monitoring Camera Video" form to the TMC Supervisor for assessment and decision-making in consultation with the PWD Director, PWD Engineer Traffic Signals, and PWD Records and Information Management Coordinator.

37 Requests to use TMC Cameras or TMC video/visual clips for external research purposes must be assessed to ensure conditions of FIPPA s.47 can be met by the requestor.

38 Research agreements must be negotiated with the aid of Legal Services when needed.

Law enforcement requests for TMC video/visual clips

39 Public bodies that collect personal information for one purpose may use or disclose that information for other purposes under limited circumstances defined in FIPPA, such as law enforcement or crime prevention per FIPPA s.44(1)(r). To ensure a use under that section of FIPPA is authorized, the following process must be followed:

(a) The law enforcement officer must submit their completed "Law Enforcement Request for Personal Information" form to the TMC Supervisor for processing. (Note: There is an exception to the requirement for the Law Enforcement Request for Personal Information Form. Where law enforcement has served a production order, it is mandatory that the records be provided to law enforcement, as directed in the order. Submit a request for consultation to the City's Legal Services department for advice on responding to production orders.

(b) Due to the automatic 7-day retention of TMC video, law enforcement officers are advised to submit their request on days 1-4 because requests received on days 5-7 are at risk of the record being overwritten.

(c) All fields on the form are mandatory and include the following: names and badge numbers of requestor and an alternate contact, case number, date and start/stop times for search, location of TMC Camera(s) for search per published list of TMC camera locations, nature of the personal information requested, offence or crime under investigation or that is the subject of crime prevention with the section of the federal or provincial statute or by-law cited, confirmation that the request is for the minimum amount of personal information necessary to accomplish the law enforcement matter.

(d) Incomplete forms cannot be processed and must be returned to the requestor as "unprocessed due to incomplete form." Forms may be resubmitted once completed.

(i) If a WPS law enforcement officer has a concern about how the request is being processed or the response they received, they must flag their concern to their Supervisor/Divisional Commander.

(ii) If the TMC Supervisor receives or has a complaint or concern, they consult with the Engineer Traffic Signals (i.e., their manager) and, if needed, the Corporate Access and Privacy Officer to determine next steps. The Engineer Traffic Signals will work to resolve the complaint or concern in consultation with the WPS Inspector for Division 11 and the Corporate Access and Privacy Officer.

40 The TMC Supervisor, or delegate, shall:

(a) Receive the request during regular TMC operational hours (Monday-Friday, 06:00-19:00) and, in addition, will check for requests once in the afternoon and once in the evening on weekends and holidays to minimize the risk of video being overwritten before a request has been received.

(i) Where the requestor marks the level of urgency as "exigent," the TMC Supervisor will try to process the request as soon as possible. Otherwise, requests will be processed during TMC's operational hours.

(b) Take the request form at face value and provide exactly what is requested, accepting the information as presented on the form as accurate; however, will clarify incorrectly identified camera locations on the form if needed.

(c) Not review TMC video for content or confirmation of details on behalf of a law enforcement officer.

(d) Transfer requested video to WPS secure site and do not keep a copy once the transfer is complete.

41 WPS records management rules and retention periods apply to the video once they receive copies of the video from TMC.

42 In conjunction with a member of the WPS Legal Counsel Unit, the Corporate Access and Privacy Officer conducts those portions of the annual Traffic Monitoring Camera Program Audit related to WPS requests for video and camera control. The audit shall evaluate compliance with relevant policies, procedures, and legislation to ensure that videos are accessed, used, and disclosed for authorized purposes, and to identify any unintended operational, technical, or privacy issues for either TMC or the WPS.

FIPPA requests

43 All other requests (public, media, union) for copies of TMC video must be managed through the process outlined in Part 2 of FIPPA for obtaining access to records in the custody or control of a public body.

44 FIPPA requests for TMC video must be submitted to the City Clerk's Department for processing. The requests are directed to the PWD Records and Information Management Coordinator for response.

(a) In consultation with the PWD Records and Information Management Coordinator, the TMC Supervisor must review and sever any third-party personal information prior to disclosure of requested TMC visual clip.

(b) There is no fee for making a FIPPA request but, if the time for searching and preparing the records will exceed 2 hours or if the request will require computer programming or data processing, a fee estimate may be issued to the applicant under FIPPA s.82 and the Access and Privacy Regulation s.4 to s.8. Fee estimates must be based on the average time such work takes, in addition to the search time.

(i) Average time for preparation of TMC visual clip: 1-hour video = 1.5 hours preparation

(ii) Average in-house data processing: 15-minute TMC visual clip = 1 hour of data processing

(iii) When in-house data processing is not possible, it may be contracted out and the fee estimate must reflect the actual cost to the City for the contracted work.

(iv) TMC visual clip will be provided in a readable video format on a memory stick. The actual cost of the memory stick is the copy cost and is payable when the applicant is provided the copy. Delivery is through regular mail at no charge, or courier delivery at the FIPPA applicant’s expense and coordination.

General enquiries

45 All enquiries from City departments are be directed to the TMC Supervisor.

46 All 311 enquiries regarding the TMC cameras program, operation or policies shall direct the inquiry to the TMC’s 311 Service Request queue.

UNAUTHORIZED USE OR DISCLOSURE

47 A privacy breach occurs when there is unauthorized access and/or disclosure of personal information about citizens or employees (in contravention of FIPPA), or that this information has been lost or stolen.

(a) A breach of this protocol by an employee of the City of Winnipeg may result in discipline, up to and including dismissal.

(b) A breach of this protocol by service providers (contractors) to The City of Winnipeg may result in a poor performance review and/or termination of their contract.

48 Any City of Winnipeg employee or contractor who becomes aware of any unauthorized use of TMC cameras or unauthorized disclosure of TMC video, this protocol and/or a potential privacy breach must notify the TMC Supervisor immediately.

49 The TMC Supervisor must immediately:

(a) Contain the breach.

(b) Report the breach to the PWD Records and Information Management Coordinator and assist with evaluating and mitigating associated risks.

(c) If required, notify impacted individuals.

50 The PWD Records and Information Management Coordinator must complete a privacy breach report and submit it to the Corporate Access and Privacy Officer as soon as possible.