City of Redmond

Redmond
WASHINGTON

Agenda

Study Session

Tuesday, March 10, 2026
7:00 PM

City Hall: 15670 NE 85th St; Remote: Comcast Ch. 21/321, Ziply Ch. 34, Facebook (@CityofRedmond), Redmond.gov/rctvlive, or 510-335-7371

City Council

Mayor
Angela Birney

Councilmembers
Melissa Stuart, President
Angie Nuevacamina, Vice President
Jessica Forsythe
Vanessa Kritzer
Sayna Parsi
Vivek Prakriya
Menka Soni

Redmond City Council Agendas, Meeting Notices, and Minutes are available on the City's Web Site: http://www.redmond.gov/CouncilMeetings

FOR ASSISTANCE AT COUNCIL MEETINGS FOR THE HEARING OR VISUALLY IMPAIRED:
Please contact the City Clerk's office at (425) 556-2194 one week in advance of the meeting.

Meetings can be attended in person, viewed live on RCTV (redmond.gov/rctvlive), Comcast Channel 21/321, Ziply Channel 34, Facebook/YouTube (@CityofRedmond), or listen live at 510-335-7371

AGENDA

ROLL CALL

1. Police Technology Update

Department: Police, 90 minutes

Attachment A: RPD Policy 341 - Public Safety Technology Data Governance
Attachment B: RPD Policy 612 - Automatic License Plate Readers
Attachment C: Keep Washington Working - RCW 10.93.160
Attachment D: WA SB 6002 - 2026
Attachment E: Flock ALPR Camera Locations

2. Draft 8th Amendment to the Council Rules of Procedure

Council, 30 minutes

Council Memo

3. Council Talk Time

10 minutes

ADJOURNMENT

Meeting videos are usually posted by 12 p.m. the day following the meeting at redmond.legistar.com, and can be viewed anytime on Facebook/YouTube (@CityofRedmond) and OnDemand at redmond.gov/OnDemand

Memorandum

Date: 3/10/2026
Meeting of: City Council

File No. SS 26-028
Type: Study Session

TO: Members of the City Council
FROM: Mayor Angela Birney
DEPARTMENT DIRECTOR CONTACT(S):

Police	Chief Darrell Lowe	425-556-2521

DEPARTMENT STAFF:

Police	Brian Coats	Deputy Chief

TITLE:
Police Technology Update

OVERVIEW STATEMENT:
The Redmond Police Department (RPD) respectfully submits this briefing to provide City Council with a comprehensive update on current and emerging public safety technologies. This communication covers the Drone as First Responder (DFR) Program, the Real-Time Information Center (RTIC), the upgrade of Redmond's existing fixed city traffic camera infrastructure, and Automated License Plate Reader (ALPR) technology including a comparison of fixed versus mobile ALPR systems, the current suspension of investigative ALPR, pending state legislation, and a recommendation for the path forward.

Every technology discussed in this briefing was adopted or is being considered through a consistent evaluative lens: Does it solve a specific public safety problem? Does it create measurable operational efficiency? Does it enhance the effectiveness and outcomes of the department's public safety mission while respecting the rights, privacy, and trust of every member of our community? That philosophy shapes every recommendation in this document.

☒ **Additional Background Information/Description of Proposal Attached**

REQUESTED ACTION:

☒ **Receive Information** ☐ **Provide Direction** ☐ **Approve**

REQUEST RATIONALE:

- **Relevant Plans/Policies:**
  DFR Program Dashboard (live): redmond.gov/2172/Drone-Program-Dashboard
- **Required:**
  N/A

- **Council Request:**
  Council request for routine updates
- **Other Key Facts:**

1. DRONE AS FIRST RESPONDER (DFR) PROGRAM

Does it solve a problem? Yes. Does it create efficiency? Yes.

Launched in April 2024, the RPD DFR program became the first full-time Drone as First Responder program in Washington State and the Pacific Northwest. Drones deploy from fixed docking stations citywide and can arrive on scene before ground units, providing aerial situational awareness to responding officers.

Demonstrated Impact

- 3,344 calls have been responded since program launch.
- Deployed in incidents involving armed individuals, DUIs, missing persons, shoplifting, traffic collisions, and structure fires.
- DFR deployed to a man-with-a-gun call at an apartment complex, providing real-time aerial intelligence that allowed officers to approach safely, assess accurately, and de-escalate - a direct officer and community safety outcome.

Pilots can cancel unnecessary ground unit responses when DFR confirms no active threat, preserving resources for priority calls.

2. REAL-TIME INFORMATION CENTER (RTIC)

Does it solve a problem? Yes. Does it create efficiency? Yes.

- The RTIC is the operational and governance hub for RPD's technology infrastructure. Trained analysts synthesize data from calls for service, camera feeds, drone video, mapping tools, and analytics platforms to support real-time decision-making during active incidents and planned events.

Operational Value

- Reduces information latency officers arrive with situational awareness rather than uncertainty.
- Enables command coordination during critical incidents and large-scale events.
- Human review is embedded at every step: no automated system triggers enforcement action without analyst confirmation.

3. FIXED CITY TRAFFIC CAMERA INFRASTRUCTURE

Does it solve a problem? Yes. Does it create efficiency? Yes.

- This section addresses the planned upgrade of Redmond's existing fixed city traffic camera infrastructure the network of cameras already in place at traffic corridors and key public spaces throughout the city. This is not a proposal to expand the number or scope of camera deployments; it is an investment in the reliability, image quality, and integration capability of infrastructure that already exists and that the community has already accepted.

Why Upgrade Now

- Aging equipment produces degraded image quality that reduces evidentiary value in investigations and limits RTIC operator effectiveness during critical incidents.
- FIFA World Cup
- Integration with the RTIC requires updated hardware capable of delivering reliable, high-resolution feeds in real time.
- Reliability gaps create operational blind spots during the incidents when camera coverage matters most.

What the Upgrade Does Not Do

- Does not expand camera coverage beyond currently approved locations.
- Does not add new surveillance capability or purposes beyond those already established.
- Does not change retention periods, access controls, or governance all remain governed by Policy 341.

4. AUTOMATED LICENSE PLATE READER (ALPR) TECHNOLOGY

Understanding the Full ALPR Landscape

- The department operates or oversees three distinct categories of ALPR technology. These must be understood separately, as they serve different purposes, operate under different legal frameworks, and carry different community implications. Council's suspension applies specifically to the investigative fixed-camera system.

System	Purpose	Mechanism	Current Status
Investigative Fixed ALPR (Flock Safety)	**Detect vehicles linked to crimes, stolen vehicles, and missing persons citywide 24/7.**	**Fixed cameras at strategic city locations always-on coverage independent of officer deployment.**	**SUSPENDED - pending Council direction.**
Mobile ALPR (In-Car Camera)	**Detect wanted vehicles during patrol opportunistic coverage dependent on officer routing.**	**Mounted on patrol vehicles active only when car is present at same location as target vehicle.**	**Available as an alternative, not currently deployed.**

Mobile ALPR (In-Car Camera)Detect wanted vehicles during patrol opportunistic coverage dependent on officer routing.Mounted on patrol vehicles active only when car is present at same location as target vehicle.Available as an alternative, not currently deployed.			
Parking Enforcement ALPR	**Enforce parking regulations and permit zones.**	**Mobile operates under separate legal framework from investigative ALPR.**	**Operational.**
School Zone Speed Enforcement	**Enforce speed limits in school zones to protect children.**	**Fixed subject-specific statutory authority.**	**Operational.**

Fixed vs. Mobile ALPR: Why Fixed Infrastructure Is the More Effective Tool

Council should be aware that mobile ALPR technology camera systems mounted on patrol vehicles exists as an alternative to the fixed Flock Safety infrastructure currently suspended. After careful evaluation, the department does not recommend mobile ALPR as a substitute. The reasons are operational and grounded in the department's evaluative framework of problem-solving and efficiency:

- Coverage dependency: Mobile ALPR can only detect a wanted vehicle if a patrol car happens to be in the same location at the same time. Fixed cameras provide continuous, citywide coverage 24 hours a day, regardless of officer deployment patterns.

- Reactive vs. proactive value: Fixed systems alert officers when a wanted vehicle enters a monitored area, allowing rapid, targeted response. Mobile systems capture plates passively during routine patrol an officer may drive past a wanted vehicle without any alert if the system is not actively querying that specific plate at that moment.

- Resource efficiency: Fixed infrastructure generates alerts without requiring an officer to be present. Mobile ALPR consumes officer time and patrol resources while delivering narrower and less reliable coverage.

- Investigative gap: A wanted vehicle associated with a felony investigation may sit in a residential neighborhood for days without a patrol car passing. Fixed cameras at key corridors capture that vehicle the moment it moves. Mobile ALPR would miss it entirely unless an officer happened to be on the same block.

In short: mobile ALPR relies on coincidence. Fixed ALPR relies on infrastructure. For a department committed to efficiency and effectiveness, fixed infrastructure is the operationally superior choice. The department

acknowledges this assessment and presents it to Council as relevant context for evaluating the suspension.

Background on the Suspension

Following reports in early 2025 of ALPR data being shared with federal immigration enforcement (ICE) in other jurisdictions without community knowledge or consent Redmond's investigative ALPR program was suspended by Council. The department fully supports Council's exercise of oversight authority. However, the community should understand that Redmond's program had already built protections that distinguished it from those where problems occurred:

- No nationwide data sharing: Redmond did not activate Flock Safety's national shared network. Data remained local.
- Chief-level approval for all external requests: Vague or ambiguous requests were denied; the investigative sergeant verified legal basis before any release.
- Documented investigative nexus required: Every officer query required a valid case number and documented nexus. No speculative searches.

Chief's Recommendation: Resume Investigative ALPR Upon Passage of SB 6002

The department respectfully but clearly recommends that Council authorize resumption of the investigative ALPR program upon enactment of SB 6002, provided Redmond's policies are updated to comply with the new state law. This recommendation is grounded in the following:

- SB 6002 directly addresses the concerns that motivated the suspension. The legislation codifies in state law what Redmond's internal policy had already established including the prohibition on immigration enforcement use and the mandatory audit requirements. The community's concern about data misuse will, upon passage, be backed by statutory penalties including criminal liability for willful violations.
- Washington State will provide a legal framework and enforcement mechanism that does not depend on any individual agency's good faith. That is the structural protection the community deserves.
- The operational case for fixed ALPR is compelling. Stolen vehicles, trafficking cases, felony suspects these are problems ALPR solves in ways that no other available tool replicates with the same speed and coverage.
- Redmond's existing safeguards no data sharing, chief-level approval, mandatory case nexus, system-level immigration filter already exceed what SB 6002 requires. Compliance will be a policy update, not a program redesign.

The department is not asking Council to accept the program as it was before suspension. It is asking Council to commit to resuming the program once the state has provided the legal structure that gives the community the assurance it deserves. The longer the suspension continues beyond that point, the greater the cost in investigations delayed, vehicles not recovered, and vulnerable residents not protected.

If the session closes without SB 6002 passing, the department recommends that Council provide direction on reinstatement under enhanced written policy rather than continued indefinite suspension.

5. TECHNOLOGY GOVERNANCE & OVERSIGHT FRAMEWORDK

All RPD technology programs operate under a unified governance structure. Relevant governing documents include:

- RPD Policy 341 - Public Safety Technology Data Governance: Standards for data collection, retention, access, auditing, and community transparency across all technology systems. Publicly available at redmond.gov.
- RPD Policy 612 - Automated License Plate Readers: Specific operational and data handling requirements for ALPR systems. Publicly available at redmond.gov.
- RCW 10.93.160 - Keep Washington Working Act: Binding state law restricting use of state resources for immigration enforcement, with which all RPD technology programs comply.
- SB 6002 (pending): Once enacted, the state will establish the first comprehensive ALPR governance statute, creating mandatory statewide standards that supersede and reinforce existing local policy.

The department also proposes establishing a regular public-facing technology transparency report annual, covering system access volume, incident categories, outcomes, and audit results to give every community member a direct window into how these tools are being used on their behalf.

OUTCOMES:

Following this briefing, the department requests that Council:

- Acknowledge receipt of the technology update and provide any immediate feedback or questions.
- Commit to authorizing resumption of the investigative ALPR program upon enactment of SB 6002, with policy updates to comply with the new state law.
- In the event SB 6002 does not pass during the current session (closing March 12, 2026), provide direction on the path forward for investigative ALPR so the department can manage equipment and communicate clearly with the community.
- Indicate any areas where Council would like additional information, independent review, or community engagement prior to future action.

COMMUNITY/STAKEHOLDER OUTREACH AND INVOLVEMENT:

- **Timeline (previous or planned):**
  N/A
- **Outreach Methods and Results:**
  N/A
- **Feedback Summary:**
  N/A

BUDGET IMPACT:

Total Cost:
No new appropriation requested at this time. Camera upgrade costs to be presented in a separate budget offer.

Approved in current biennial budget: ☐ **Yes** ☐ **No** ☒ **N/A**

Budget Offer Number:
228

Budget Priority:
Safe and Resilient

Other budget impacts or additional costs: ☐ **Yes** ☐ **No** ☒ **N/A**
If yes, explain:
N/A

Funding source(s):
General Fund

Budget/Funding Constraints:
The continued suspension of investigative ALPR represents an ongoing cost in equipment maintenance and unquantified investigative capability loss. A fiscal impact analysis is available upon Council's request.

☐ **Additional budget details attached**

COUNCIL REVIEW:

Previous Contact(s)

Date	Meeting	Requested Action
10/21/2025	Committee of the Whole - Public Safety and Human Services	Receive Information

Proposed Upcoming Contact(s)

Date	Meeting	Requested Action
N/A	None proposed at this time	N/A

Time Constraints:
N/A

ANTICIPATED RESULT IF NOT APPROVED:
N/A

ATTACHMENTS:
Attachment A: RPD Policy 341- Public Safety Technology Data Governance
Attachment B: RPD Policy 612 - Automated License Plate Readers (attached)

Attachment C: Keep Washington Working Act (full text)
Attachment D: Enrolled Senate Bill (current version as of February 2026)
Attachment E: Investigative ALPR Camera Location Map

Public Safety Technology Data Governance

Effective Date:	July 2025
Revised Date:	
Issuing Authority:	

341.1 PURPOSE AND SCOPE

The Redmond Police Department is committed to the responsible and ethical use of technology. The purpose of this policy is to establish guidelines for the use of data gathered and generated by the different public safety technologies deployed by the Redmond Police Department. This policy aims to ensure that the deployment and utilization of these technologies are conducted in a manner that respects privacy, civil liberties, and public trust and are consistent with state law, city policy and WASPC accreditation standards.

The department shall maintain transparency in the use of public safety technologies and inform the public about their purposes, capabilities, and the safeguards in place to protect individual rights.

Officers and personnel involved in the use of these technologies will be held accountable for their actions and adherence to this policy. Violations will result in disciplinary action, up to and including termination, in accordance with departmental procedures, City policy, and collective bargaining agreements.

341.2 POLICY

Public safety technology (PST) data will be used solely for law enforcement purposes. Any non-law enforcement usage of PST data is strictly prohibited. PST data will not be used to intentionally monitor private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate, or discriminate against any individual or group.

PST systems will only be deployed for official law enforcement purposes and will only be accessed by trained, RPD employees. This access is limited to search of specific information related to any of the following:

- Criminal investigations
- Searches for wanted persons or persons of interest
- Community caretaking functions, such as locating an endangered or missing person

Employees will only use PST data pursuant to this policy and applicable city, state, and federal laws.

This policy will be reviewed regularly to ensure it remains current and consistent with technological advancements, legal requirements, best practices in data governance, and City policy.

341.3 POLICIES AND OPERATING PROCEDURES FOR SPECIFIC TECHNOLOGIES

The Redmond Police Department will adopt policies to provide specific guidance for deployment and operation of the different technologies in use. Those individual policies will follow and refer to this data governance policy. These programs include but are not limited to:

- Drones including Drone as a First Responder (DFR)
- Automatic License Plate Readers (ALPR)
- Speed Safety Cameras
- In-car and Body-Worn Video
- Technologies used by the Real Time Information Center (RTIC)

341.4 STORAGE AND RETENTION OF DATA

The department and city have robust security measures currently in place in compliance with CJIS data security, and the cities cyber-insurance carrier requirements to protect the data from unauthorized access or breaches.

Generally, PST systems store data from the various technologies no longer than 30 days. After the 30-day period, the data will be purged unless it related to an ongoing investigation or legal requirement. In those circumstances, the applicable data should be downloaded from the server and entered into evidence.

Detectives will retain PST data related to a criminal investigation in the investigation case file for a period in accordance with state retention laws.

341.5 REVIEW OF PST DATA

Only authorized personnel may access PST data and only in conjunction with a call for service or investigation. Employees accessing PST data must log in through password-protected systems.The systems record when an employee accesses the data by logging the employee's name, the date, and the time of the request. Employees will not share PST passwords and login credentials.

Employees conducting searches will provide a case number and justification for the search. If a case number does not exist, the employees will provide thorough justification for the legitimacy and lawful purpose of the search.

Regular audits will be conducted to ensure compliance with this policy.

341.6 RELEASING OR SHARING OF PST DATA

PST data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. In addition, the Redmond Police Department will only share PST data with other agencies when the investigation relates to a violation of Washington State Law or is tied to the City of Redmond. The Redmond Police Department will not share PST data with other agencies for the purpose of locating or tracking

persons wanted solely for administrative reasons, such as immigration law violations, or for violations in other jurisdictions that would not otherwise warrant investigation in Redmond.

Requests for PST data by non-law enforcement or non-prosecutorial agencies will be processed by the Records Unit pursuant to the applicable Rules of Civil or Criminal Discovery or the Washington Public Records Act, Ch. 42.56 RCW.

341.7 TRAINING

Before employees operate the various PST systems, they will complete department training on the proper and lawful use of the system. The Training Unit will coordinate with the appropriate program or system administrator to provide this training.

The training will emphasize proper use, data handling procedures, ethical considerations outlined in this policy, and the requirement to document the reason for any data inquiry.

Additionally, all RPD employees with access to PST data will maintain ACCESS Level 1 Certification pursuant to ACCESS WACIC and NCIC.

The PST program administrators will maintain a list of all employees trained in the use of the equipment and systems and update user access.

341.8 PUBLIC REPORTING

The department will engage in community outreach and education efforts to inform the public about the use of these public safety technologies, their benefits, and the safeguards in place to protect privacy and civil liberties.

The department will include in its published annual report details on the use of public safety technologies, including data on their deployment, effectiveness, and any privacy or civil liberties issues encountered.

Any incidents of misuse or abuse of these technologies will be handled in accordance with established department policy, state law, and accreditation standards reporting requirements.

Automatic License Plate Readers

Effective Date:	July 2025
Revised Date:	
Issuing Authority:	

612.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the responsible and ethical use of Automated License Plate Readers by the Redmond Police Department. This policy aims to ensure that the deployment and utilization of these technologies are conducted in a manner that respects privacy, civil liberties, and public trust and are consistent with state law, city policy and WASPC accreditation standards.

Automatic License Plate Readers (ALPRs) use cameras to photograph vehicles and license plates. ALPR technologies used by the Redmond Police Department include vehicle-mounted cameras and stationary cameras installed in strategic locations around the city. This technology is for authorized law enforcement and public safety purposes as set forth in this policy.

This policy applies to the use of ALPRs and associated information by all department employees. This policy governs the use of ALPR data, to enable the collection and use of such data in a manner consistent with respect for individuals' privacy and civil liberties.

This policy is intended to provide guidance specific to ALPR systems and is in addition to the provisions found in the department's Public Safety Technology Data Governance Policy 341.

This policy will be reviewed regularly to ensure it remains current and consistent with technological advancements, legal requirements, best practices in data governance, and City policy.

612.1.1 DEFINITIONS

ALPR Administrator: A Department employee who manages the utilization of the ALPR software from the end user through training, reporting, and monitoring.

Hit: Alert from the ALPR system that a scanned license plate number may be in the NCIC or other law enforcement database for a specific reason including, but not limited to, being related to a stolen vehicle, wanted person, missing person, domestic violence protective order, or other criminal activity.

Hot List: A collection of license plates associated with vehicles of interest from databases that include, but not limited to: National Crime Information Center (NCIC), Washington Crime Information Center (WACIC), Department of Licensing (DOL) databases, and local "be on the lookout" notices (BOLOs).

Reads: Data obtained by an ALPR of license plates within public view that were read by the device, including images of the plate and vehicle on which it was displayed, and information regarding the location of the police vehicle at the time of the ALPR read.

612.2 POLICY

ALPR systems will only be deployed for official law enforcement purposes. Examples of these include:

- Locating stolen vehicles and stolen license plates
- Locating wanted, endangered or missing persons; or those violating protection orders
- Canvassing the area around a crime scene

ALPR data will only be accessed by RPD employees for official law enforcement purposes such as:

- Criminal investigations
- Searches for wanted persons or persons of interest
- Community caretaking functions, such as locating an endangered or missing person

Before employees operate the ALPR system or access its data, they will complete department training on the proper and lawful use of the system. The Training Unit will coordinate with the ALPR Administrator to provide this training.

612.2.1 CUSTOM HOTLISTS

Users who create custom hotlists will include the following information for each entry:

- Case number
- Topic explaining the nature of the investigation
- Comments detailing the reason for the contact (e.g. PC for Arrest, Identify Driver, etc.) if the list is shared or the audience includes anyone other than the person who created the entry.
- Reasonable expiration date for the entry

Users are responsible for maintaining their custom hotlists and promptly removing entries that are no longer necessary.

612.3 OPERATING ALPR SYSTEMS

ALPR operators will activate the software and ensure that it is operational at the beginning of their shift. Operators will notify the ALPR Administrator upon discovery of any damaged or inoperable ALPR equipment.

ALPR systems automatically update hotlists.

When an operator receives a hit/alert indicating a positive hit from the hotlist database, a digital image of the license plate will display on the screen.

ALPR operators will compare the digital image of the license plate to the hotlist information to verify the hit for both the state and characters on the plate.

ALPR operators will confirm the information by radio or Mobile Data Computer (MDC) to confirm the hit prior to taking enforcement action or other type of police action (absent exigent circumstances).

The system will upload ALPR data accumulated from the shift.

612.4 DATA COLLECTION AND GOVERNANCE

ALPR technology collects digital images of license plates and associated license plate numbers. The technology collects the date and time that the license plate passes an ALPR camera. No additional personally identifiable information is collected.

Access, storage, use, and sharing of ALPR data is addressed in the Public Safety Technology Data Governance Policy 341.

RCW 10.93.160

Immigration and citizenship status—Law enforcement agency restrictions.

(1) The definitions contained in RCW 43.17.420 apply to this section.

(2) The legislature finds that it is not the primary purpose of state and local law enforcement agencies or school resource officers to enforce civil federal immigration law. The legislature further finds that the immigration status of an individual or an individual's presence in, entry, or reentry to, or employment in the United States alone, is not a matter for police action, and that United States federal immigration authority has primary jurisdiction for enforcement of the provisions of Title 8 U.S.C. dealing with illegal entry.

(3) School resource officers, when acting in their official capacity as a school resource officer, may not:

(a) Inquire into or collect information about an individual's immigration or citizenship status, or place of birth; or

(b) Provide information pursuant to notification requests from federal immigration authorities for the purposes of civil immigration enforcement, except as required by law.

(4) State and local law enforcement agencies may not:

(a) Inquire into or collect information about an individual's immigration or citizenship status, or place of birth unless there is a connection between such information and an investigation into a violation of state or local criminal law; or

(b) Provide information pursuant to notification requests from federal immigration authorities for the purposes of civil immigration enforcement, except as required by law.

(5) State and local law enforcement agencies may not provide nonpublicly available personal information about an individual, including individuals subject to community custody pursuant to RCW 9.94A.701 and 9.94A.702, to federal immigration authorities in a noncriminal matter, except as required by state or federal law.

(6)(a) State and local law enforcement agencies may not give federal immigration authorities access to interview individuals about a noncriminal matter while they are in custody, except as required by state or federal law, a court order, or by (b) of this subsection.

(b) Permission may be granted to a federal immigration authority to conduct an interview regarding federal immigration violations with a person who is in the custody of a state or local law enforcement agency if the person consents in writing to be interviewed. In order to obtain consent, agency staff shall provide the person with an oral explanation and a written consent form that explains the purpose of the interview, that the interview is voluntary, and that the person may decline to be interviewed or may choose to be interviewed only with the person's attorney present. The form must state explicitly that the person will not be punished or suffer retaliation for declining to be interviewed. The form must be available at least in English and Spanish and explained orally to a person who is unable to read the form, using, when necessary, an interpreter from the district communications center "language line" or other district resources.

(7) An individual may not be detained solely for the purpose of determining immigration status.

(8) An individual must not be taken into custody, or held in custody, solely for the purposes of determining immigration status or based solely on a civil immigration warrant, or an immigration hold request.

(9)(a) To ensure compliance with all treaty obligations, including consular notification, and state and federal laws, on the commitment or detainment of any individual, state and local law enforcement agencies must explain in writing:

(i) The individual's right to refuse to disclose their nationality, citizenship, or immigration status; and

(ii) That disclosure of their nationality, citizenship, or immigration status may result in civil or criminal immigration enforcement, including removal from the United States.

(b) Nothing in this subsection allows for any violation of subsection (4) of this section.

(10) A state and local government or law enforcement agency may not deny services, benefits, privileges, or opportunities to individuals in custody, or under community custody pursuant to RCW 9.94A.701

and 9.94A.702, or in probation status, on the basis of the presence of an immigration detainer, hold, notification request, or civil immigration warrant, except as required by law or as necessary for classification or placement purposes for individuals in the physical custody of the department of corrections.

(11) No state or local law enforcement officer may enter into any contract, agreement, or arrangement, whether written or oral, that would grant federal civil immigration enforcement authority or powers to state and local law enforcement officers, including but not limited to agreements created under 8 U.S.C. Sec. 1357(g), also known as 287(g) agreements.

(12)(a) No state agency or local government or law enforcement officer may enter into an immigration detention agreement. All immigration detention agreements must be terminated no later than one hundred eighty days after May 21, 2019, except as provided in (b) of this subsection.

(b) Any immigration detention agreement in effect prior to January 1, 2019, and under which a payment was made between July 1, 2017, and December 31, 2018, may remain in effect until the date of completion or December 31, 2021, whichever is earlier.

(13) No state or local law enforcement agency or school resource officer may enter into or renew a contract for the provision of language services from federal immigration authorities, nor may any language services be accepted from such for free or otherwise.

(14) The department of corrections may not give federal immigration authorities access to interview individuals about federal immigration violations while they are in custody, except as required by state or federal law or by court order, unless such individuals consent to be interviewed in writing. Before agreeing to be interviewed, individuals must be advised that they will not be punished or suffer retaliation for declining to be interviewed.

(15) Subsections (3) through (6) of this section do not apply to individuals who are in the physical custody of the department of corrections.

(16) Nothing in this section prohibits the collection, use, or disclosure of information that is:

(a) Required to comply with state or federal law; or

(b) In response to a lawfully issued court order.

[2019 c 440 s 6.]

NOTES:

Findings—Construction—Conflict with federal requirements—Effective date—2019 c 440: See notes following RCW 43.17.425.

ENGROSSED SUBSTITUTE SENATE BILL 6002

State of Washington 69th Legislature 2026 Regular Session

By Senate Law & Justice (originally sponsored by Senators Trudeau, Holy, Alvarado, Bateman, Chapman, Conway, Dhingra, Frame, Hasegawa, Kauffman, Lovelett, Nobles, Pedersen, Shewmake, Slatter, Stanford, and Valdez)

READ FIRST TIME 01/23/26.

AN ACT Relating to driver privacy protections and automated license plate reader systems; adding a new chapter to Title 10 RCW; prescribing penalties; and declaring an emergency.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec. 1.** INTENT. The legislature finds that it plays an important role balancing the need to ensure public safety and an individual's right to privacy under both the federal Fourth Amendment to the United States Constitution and the broader protection of individual rights guaranteed by Article I, section 7 of the Washington state Constitution.

The legislature further finds that the dramatic expansion of surveillance technology across the country has demonstrated the need to establish sensible guardrails on the use of surveillance data collected from monitoring the location and travel of individuals, without a warrant, to ensure its use by law enforcement and other government agencies must not come into conflict with existing protections for Washingtonians and ensure that it is not being used for purposes prohibited under state and federal law.

NEW SECTION. **Sec. 2.** DEFINITIONS. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Agency" includes all state agencies and all local agencies.

(2) "Audit trail" means all records of queries and responses in an automated license plate reader system, and all records of actions in which system data is accessed, entered, updated, shared, or disseminated, including the:

(a) Location of cameras used as part of the automated license plate reader system;

(b) Date and time of access;

(c) Data elements used to query the automated license plate reader system;

(d) Specific purpose for accessing or querying the automated license plate reader system, including the offense type for any criminal investigation;

(e) Associated call for service or case number; and

(f) Username of the person or persons who accessed or queried the system.

(3) "Audit trail data" means all forms of data collected or generated by an automated license plate reader system for purposes of producing an audit trail.

(4) "Automated license plate reader data" means all data collected by automated license plate reader systems including, but not limited to, global positioning system coordinates, location, date and time, speed of travel, photograph, license plate number, automobile characteristics, or other identifying information.

(5) "Automated license plate reader system" or "ALPR" means a system, software, or computer algorithm, whether used independently or in combination with one or more mobile or fixed automated cameras, that is used to convert images of license plates into computer-readable data. An ALPR excludes automated traffic safety cameras authorized under RCW 46.63.180, 46.63.200, or 46.63.220 through 46.63.260 that do not interface or interact with an ALPR system and photo toll system cameras authorized under RCW 47.56.795 or 47.46.105.

(6) "Court order," "warrant," or "subpoena" means a court order as defined in RCW 43.17.420.

(7) "Law enforcement agency" has the same meaning as in RCW 10.116.010.

(8) "Local agency" includes every county, city, town, municipal corporation, quasi-municipal corporation, special purpose district, local housing authorities, or any office, department, division, bureau, board, commission, or agency thereof, or other local public agency including their respective employees and agents.

(9) "State agency" includes every state office, department, division, bureau, board, commission, or other state agency, and their respective employees and agents.

(10) "Watch list" means a list of license plate numbers to be compared against a license plate number obtained from an automated license plate reader system.

NEW SECTION. **Sec. 3.** OPERATION. (1) Except as provided for in this section, it is unlawful for any agency to access, operate, or use an automated license plate reader system or its associated automated license plate reader data.

(2) An agency may access, operate, or use an automated license plate reader system and its associated data only for the following authorized purposes:

(a) Any law enforcement agency may use an automated license plate reader system for the purpose of comparing captured automated license plate reader data with:

(i) Data on any of the following watch lists maintained by either a federal or Washington state agency: The department of licensing, the state criminal justice information system, the federal bureau of investigation kidnappings and missing persons list, and the Washington missing persons list; or

(ii) License plate numbers that have been entered into a state or local automated license plate reader system database, upon an officer's determination that the license plate numbers are relevant and material to an investigation of a vehicle that is:

(A) Stolen;

(B) Associated with a missing or endangered person;

(C) Registered to an individual for whom there is an outstanding felony warrant; or

(D) Related to or involved in a felony.

(b) Any parking enforcement agency including, but not limited to, the department of enterprise services and institutions of higher education as defined in RCW 28B.10.016 may use an automated license plate reader system for the following purposes:

(i) Enforcing time restrictions on the use of parking spaces; or

(ii) Identifying vehicles on a watch list for impoundment or immobilization under a local ordinance enacted under RCW 46.55.240, provided the list includes only license plates of vehicles subject to that ordinance.

(c) Any transportation agency may use an automated license plate reader system for the following purposes:

(i) Providing real-time traffic information to the public, traffic modeling, and traffic studies such as determining construction delays and route use; and

(ii) Enforcing commercial vehicle systems at Washington state patrol enforcement sites and weigh stations.

(d) State and local agencies operating ALPR systems are the legal owners of the associated ALPR data.

(3) It is unlawful for any agency, as described in RCW 43.17.425, to use an automated license plate reader system for immigration investigation or enforcement, or both, in accordance with RCW 10.93.160, or for any protected health care services under chapter 7.115 RCW, or to track or otherwise monitor activity protected by the Washington state Constitution and the first amendment to the United States Constitution.

(4) It is unlawful for any agency to collect automated license plate reader data on the premises or immediate surroundings or access to or from facilities that provide protected health care, as described in chapter 7.115 RCW, or at facilities conducting an immigration matter as defined in RCW 19.154.020, schools, places of worship, courts, or food banks.

(5)(a) Any agency that intends to use, or currently uses an ALPR system as of the effective date of this section and intends to continue using the system, shall register it with the office of the attorney general on forms approved by the office for that purpose within 180 days of the effective date of this section. The head of the agency shall certify that the system meets all the requirements of this chapter, and that the agency has a policy or policies in effect governing its use and a documented training process for the officers that will use it. Agencies may not use ALPR systems that have not been properly registered under this section.

(6) A positive match by an automated license plate reader system alone does not constitute reasonable suspicion as grounds for a state or local law enforcement officer to stop the vehicle. The officer

shall develop independent reasonable suspicion for the stop or immediately confirm visually that the license plate on the vehicle matches the image of the license plate displayed on the automated license plate reader system and confirm by other means that the license plate number is on one of the lists specified in subsection (2)(a) of this section.

NEW SECTION. **Sec. 4.** RETENTION. Automated license plate reader data collected by or on behalf of an agency, as authorized pursuant to section 3(2) of this act, shall not be used or shared for any other purpose and shall not be retained longer than 21 days, with the following exceptions:

(1) When retained pursuant to a valid, court-issued, probable cause felony warrant or subpoena, or as permitted by court order in criminal or civil cases, provided the data is deleted at the conclusion of the criminal or civil case. ALPR data may be shared in discovery in accordance with applicable court rules;

(2) When retained for the purpose of parking enforcement, provided the data is deleted no later than 12 hours after collection;

(3) When retained for the purpose of traffic studies, provided the data is deleted no later than 30 days after collection;

(4) When retained for the purpose of enforcing commercial vehicle systems, provided the data is deleted no later than four hours after collection; and

(5) When retained for the purpose in section 3(2)(a) of this act for as long as such captured ALPR data is needed as evidence of specific unlawful conduct enumerated in section 3(2)(a) of this act.

NEW SECTION. **Sec. 5.** PROHIBITED PRACTICES. (1) An agency that uses an automated license plate reader system pursuant to section 3(2) of this act shall not:

(a) Disclose, share, or permit access to automated license plate reader data except as required in a judicial proceeding;

(b) Provide any other entity with direct access to the automated license plate reader system, except with other state or local agencies authorized to collect ALPR data under section 3 of this act. A third-party vendor providing ALPR services may directly access an ALPR system and data.

(2) Any agency that uses a watch list pursuant to section 3(2)(a) and (b)(ii) of this act must ensure the watch list is updated no less than once every 24 hours.

(3) An agency shall not sell, lease, rent, or purchase automated license plate reader data or audit trail data.

(4) An agency may obtain privately held automated license plate reader data only pursuant to a valid, court-issued, probable cause warrant.

(5) Automated license plate reader data is not subject to disclosure under the public records act, chapter 42.56 RCW, except such data may be used for bona fide research as defined in RCW 42.48.010 and does not include individually identifiable information.

(6) Any ALPR vendor must provide technical controls preventing unauthorized data sharing, secondary transfer, or access by nonauthorized agencies, including federal civil immigration enforcement in accordance with this chapter.

(7) ALPR vendors are prohibited from selling, leasing, renting, or otherwise allowing access to ALPR data to any nonauthorized agency, person, or entity.

(8) An ALPR vendor is prohibited from making any changes to an ALPR system, including but not limited to software updates that may change sharing permissions, without the knowledge or explicit consent of the authorized Washington agency. ALPR vendors must default any settings related to sharing to prevent any sharing of an agency's data with any nonauthorized agency, person, or entity.

NEW SECTION. **Sec. 6.** RECORDKEEPING/LOG. If an ALPR operator accesses or provides access to ALPR data, the ALPR operator shall do both of the following:

(1) Maintain a record of that access for five years. At a minimum, the record must include all of the following:

(a) The date and time the data is accessed;

(b) Data elements used to query the ALPR system;

(c) The username of the person who accesses the data and, as applicable, the organization or entity with whom the person is affiliated;

(d) The purpose for accessing the data;

(2) Require that ALPR data only be used for the authorized purposes in this act.

NEW SECTION. **Sec. 7.** ADMISSIBILITY IN COURT. Any information obtained from a knowing violation of section 3 of this act is inadmissible in any civil or criminal case in all courts of general or limited jurisdiction in this state, except with the permission of the person whose rights have been violated in an action brought for damages under section 11 of this act.

NEW SECTION. **Sec. 8.** POLICIES. (1) By July 1, 2027, the attorney general shall develop and publish model policies on the use of automated license plate reader systems consistent with this act.

(2)(a) By December 1, 2027, any agency that uses an automated license plate reader system pursuant to section 3(2) of this act shall:

(i) Adopt a policy governing use of the automated license plate reader system consistent with the model policies established under subsection (1) of this section and submit copies of the applicable policies to the attorney general; or, if the agency did not adopt policies consistent with the model policies, provide notice to the attorney general stating the reasons for any departures from the model policies and an explanation of how the agency's policies are consistent with the provisions of this act, and include a copy of the agency's relevant policies; and

(ii) Submit an annual report on its automated license plate reader system practices and usage to the appropriate committees of the legislature. The report must also be conspicuously posted on the agency's public website. The report shall include:

(A) The number of matches that resulted in arrest and prosecution;

(B) The number of stolen vehicles and stolen license plates recovered due to use of the system;

(C) The number of preservation requests and disclosure orders received;

(D) The number of times automated license plate reader data or audit trail data was shared with or accessed by another governmental entity and the identity of each of those governmental entities;

(E) The number of times automated license plate reader data was shared or accessed pursuant to a judicial warrant;

(F) Any changes in policy that affect data collection, retention period, access or sharing;

(G) Results from the agency's internal audit of its ALPR system; and

(H) The total annual number of ALPR reads, hits, matches, and alerts.

(b) Prior to or coincident with implementation of an automated license plate reader system, a local law enforcement agency shall take measures to promote public awareness on the use of such system.

(3) After December 1, 2026, whenever an agency modifies or repeals any policies pertaining to the use of automated license plate reader systems, the agency shall submit notice of such action with copies of any relevant policies to the attorney general within 60 days.

(4) By December 31, 2027, the attorney general shall publish on its website a report on the requirements of this section, including copies of the model policies.

(5) Agencies that adopt policies required by this section must publish the policies on the agency website and submit a website link for those published policies with the attorney general. The attorney general is not required to publish those agency policies.

NEW SECTION. **Sec. 9.** AUDITS. (1) Each agency operating or accessing an automated license plate reader system shall maintain audit trail data documenting all access to and use of the system. Audit trail data must be retained for two years and must include, at a minimum:

(a) The identity of each user and the date, time, and purpose of each system access or search;

(b) Search term entered, where applicable;

(c) Any export, download, or sharing of ALPR data; and

(d) Any audit trail data generated by or made available through a third-party vendor providing ALPR services. Each agency shall ensure that all such vendor audit trail data is downloaded or otherwise obtained and retained by the agency in accordance with this section.

(2) Each agency shall conduct an internal audit at least once each year to review:

(a) All access to and use of the ALPR system, as reflected in the audit trail data; and

(b) The agency's compliance with the data retention, purging, and sharing requirements established under this chapter and agency policy.

NEW SECTION. **Sec. 10.** VIOLATIONS—APPLICATION OF THE CONSUMER PROTECTION ACT. (1) The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW.

(2) This section applies only to persons, as defined in RCW 19.86.010, who enter into contract with state and local government agencies authorized to use ALPR systems.

NEW SECTION. **Sec. 11.** CRIMINAL PENALTIES. Any person who willfully and intentionally queries, accesses, or uses an automated license plate reader system for a purpose not specifically authorized under this chapter, or who willfully and intentionally retains, sells, shares, permits access, or disseminates automated license plate reader system data or audit trail data in violation of this chapter, is guilty of a gross misdemeanor.

NEW SECTION. **Sec. 12.** CIVIL REMEDY. A person injured by a violation of this chapter may bring a civil action to recover any equitable, declaratory relief, or injunctive relief with respect to the violation; and recover all other appropriate relief, including monetary damages. The court may award to a person aggrieved by a violation of this chapter who prevails in an action brought under this section the costs of the action, including reasonable attorneys' fees.

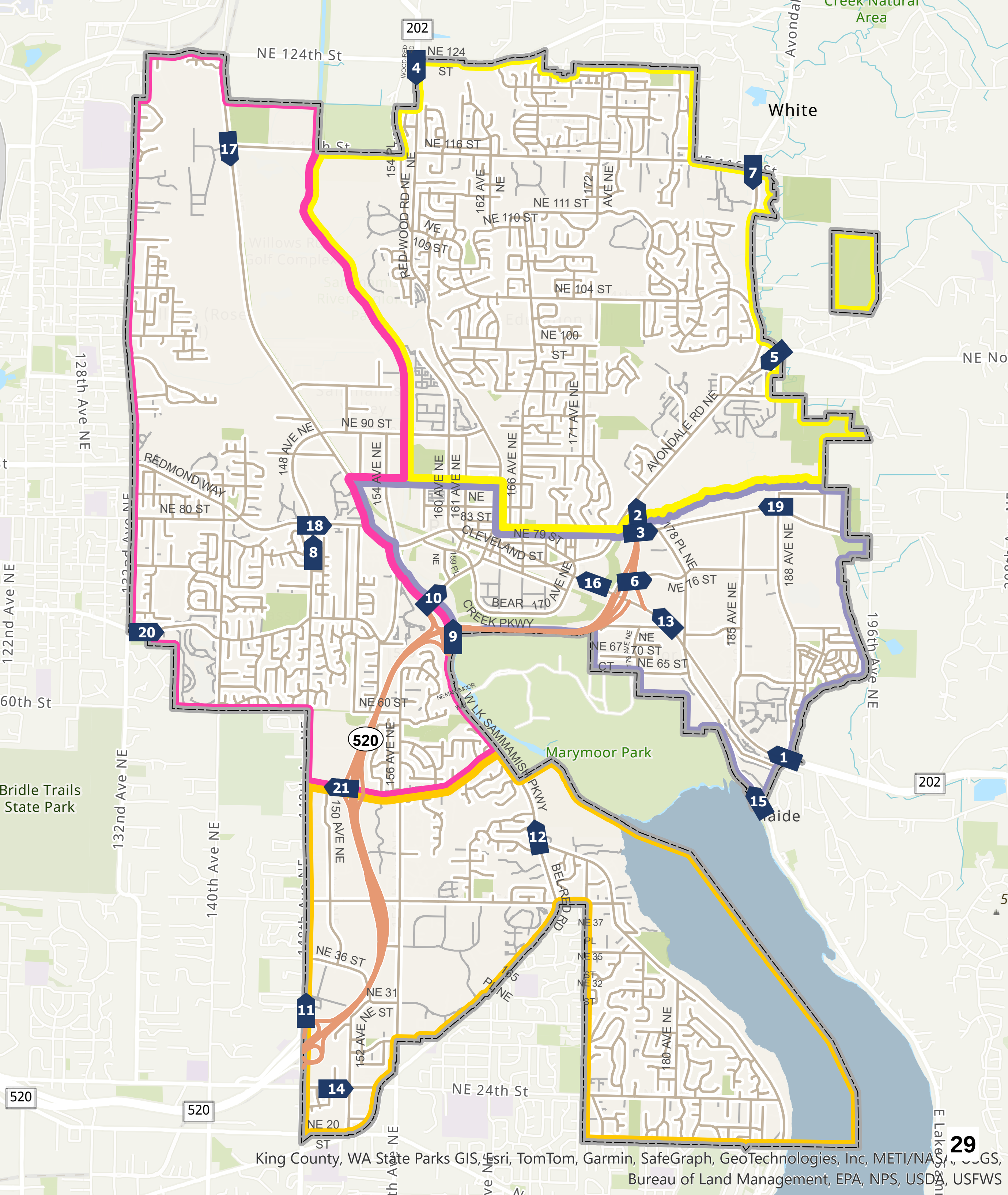
NEW SECTION. **Sec. 13.** SEVERABILITY CLAUSE. If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

NEW SECTION. **Sec. 14.** Sections 1 through 12 of this act constitute a new chapter in Title 10 RCW.

NEW SECTION. **Sec. 15.** This act is necessary for the immediate preservation of the public peace, health, or safety, or support of

the state government and its existing public institutions, and takes effect immediately.

--- END ---



NE 124th St
202
NE 124 ST
NE 116 ST
NE 111 ST
NE 110 ST
NE 109 ST
NE 104 ST
NE 100 ST
NE 90 ST
NE 83 ST
NE 80 ST
NE 79 ST
NE 76 ST
NE 70 ST
NE 65 ST
NE 60 ST
NE 36 ST
NE 31 ST
NE 20 ST
NE 24th St
REDMOND WAY
CLEVELAND ST
BEAR CREEK PKWY
AVONDALE RD NE
RED-WOOD RD NE
W LK SAMMAMISH PKWY
BEL-RED RD
148 AVE NE
150 AVE NE
154 AVE NE
156 AVE NE
160 AVE NE
161 AVE NE
162 AVE NE
166 AVE NE
171 AVE NE
172 AVE NE
178 PL NE
180 AVE NE
185 AVE NE
188 AVE NE
196th Ave NE
122nd Ave NE
128th Ave NE
132nd Ave NE
140th Ave NE
60th St
White
Marymoor Park
Bridle Trails State Park
520
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
King County, WA State Parks GIS, Esri, TomTom, Garmin, SafeGraph, GeoTechnologies, Inc, METI/NASA, USGS, Bureau of Land Management, EPA, NPS, USDA, USFWS

Flock #	Location
1	Redmond-Fall City Rd NE @ 188th Ave NE (WB)
2	Avondale Rd @ NE Union Hill Rd (NB)
3	520 @ NE Union Hill Rd (WB)
4	Redmond - Woodinville Rd @ 124th St (SB)
5	187th Court NE @ NE Novelty Hill Rd (SB)
6	NE 76th St @ 180th Ave NE (WB)
7	Avondale Rd NE @ NE 116th St (SB)
8	148th Ave NE @ NE 75th St (NB)
9	W Lake Sammamish Pkwy NE @ Hwy 520 Off Ramp (NB)
10	Leary Ave @ W. Lake Sammamish Pkwy NE (NB)
11	148th Ave NE @ NE 31st St (NB)
12	W Lake Sammamish Pkwy @ Bel-Red Rd (NB)
13	Redmond Way @ NE 70th St (NB)
14	151st St NE @ NE 24th St (EB)
15	E Lake Sammamish Pkwy @ 187th Ave NE (NB)
16	Redmond Way @ 170th Ave NE (WB)
17	Willows Rd NE @ NE 116th St (SB)
18	Redmond Way @ 148th Ave NE (EB)
19	188th Ave NE @ NE Union Hill (WB)
20	Old Redmond Rd @ NE 69th Way (EB)
21	NE 51st St @ 520 (WB)

Memorandum

Date: 3/10/2026
Meeting of: City Council

File No. SS 26-027
Type: Study Session

Draft 8th Amendment to the Council Rules of Procedure

TO: Members of the City Council
FROM: Councilmembers Stuart, Nuevacamina, and Kritzer

ASSISTING DEPARTMENT STAFF:

Executive	Cheryl Xanthos	City Clerk

TITLE:

Draft 8th Amendment to the Council Rules of Procedure

OVERVIEW STATEMENT:
Per Council direction in December 2025, Councilmembers Stuart, Nuevacamina, and Kritzer worked with the Clerk's office to prepare amendments to the Rules of Procedure on selected topics. The approved topics included issues of attendance, subcommittee management, and procedures for filling Council vacancies.

This study session time is being held in the event that further topics of deliberation are identified at the March 3 Committee of the Whole. If no topics are identified at the March 3 Committee of the Whole, then this discussion will not proceed.

☐ **Additional Background Information/Description of Proposal Attached**

REQUESTED ACTION:

☐ **Receive Information** ☒ **Provide Direction** ☐ **Approve**

REQUEST RATIONALE:

- **Relevant Plans/Policies:**
  Council Rules of Procedure
- **Required:**
  N/A
- **Council Request:**
  December 9, 2025 study session – Council Talk Time
- **Other Key Facts:**
  At the February 24, 2026 study session, Council reviewed a matrix of the proposed changes. The decisions made during that conversation are reflected in the attached and updated matrix. The Council met during the March 3 Committee of the Whole to identify any further topics of deliberation.

OUTCOMES:

The intent of these amendments is to integrate improvements to Council management and accountability, including the subcommittee management which Council provided direction for at its February 2025 retreat.

COMMUNITY/STAKEHOLDER OUTREACH AND INVOLVEMENT:

- **Timeline (previous or planned):**
  N/A
- **Outreach Methods and Results:**
  N/A
- **Feedback Summary:**
  N/A

BUDGET IMPACT:

Total Cost:
N/A

Approved in current biennial budget: ☐ **Yes** ☐ **No** ☒ **N/A**

Budget Offer Number:
N/A

Budget Priority:
N/A

Other budget impacts or additional costs: ☐ **Yes** ☐ **No** ☒ **N/A**
If yes, explain:
N/A

Funding source(s):
N/A

Budget/Funding Constraints:
N/A

☐ **Additional budget details attached**

COUNCIL REVIEW:

Previous Contact(s)

Date	Meeting	Requested Action
2/10/2026	Committee of the Whole - Finance, Administration, and Communications	Provide Direction

2/24/2026	Study Session	Provide Direction
3/3/2026	Committee of the Whole - Planning and Public Works	Provide Direction

Proposed Upcoming Contact(s)

Date	Meeting	Requested Action
4/7/2026	Business Meeting	Approve

Time Constraints:
N/A

ANTICIPATED RESULT IF NOT APPROVED:
N/A

ATTACHMENTS:
N/A

Memorandum

Date: 3/10/2026
Meeting of: City Council Study Session

File No. SS 26-029
Type: Study Session

Council Talk Time