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.