GENERAL ORDER

Oak Creek Police Department

General Order #	Applicability
26-1	All Employees

Title	From	Effective Date
USE OF INVESTIGATIVE TOOLS	Captain Andrew Thorne	August 24, 2026
	Authorized By Chief David R. Stecker	**Revision Date**

PURPOSE

To establish controls for the lawful, ethical, secure, and accountable use of investigative technology by the Oak Creek Police Department. This general order is intended to protect constitutional rights, preserve public trust, maintain evidentiary integrity, and ensure that technology is used only for legitimate law-enforcement purposes.

ORDER / PROCEDURE

This order applies to all Oak Creek personnel who have access to investigative tools. Volunteers, interns, or guests may be witnesses to investigative tools while in our facility, but they are not permitted to use them.

Members of the Oak Creek Police Department do use investigative technology during their legitimate course of business. Investigative tools shall not replace our personnel's independent judgement, legal analysis, objective reasonability, or legal responsibilities. All responses from investigative tools shall be treated as investigative leads only and should be independently corroborated and lawfully obtained.

Permitted Uses:

- Investigating criminal offenses and identifying suspects, witnesses, victims, missing or endangered people;
- Locating fugitives, escaped prisoners, or persons subject to lawful arrest;
- Supporting active search-and-rescue, disaster response, and emergency operations;
- Conducting threat assessments tied to specific public safety concerns;
- Preserving, processing, reviewing, or authenticating evidence;
- Conducting authorized intelligence or analytical functions;
- Meeting legal discovery, disclosure, records-management, and audit obligations

Members shall not use investigative technology to target, monitor, investigate, or interfere with persons based solely on actual or perceived race, color, national origin, ancestry, religion, sex, gender identity, sexual orientation, disability, age, housing status, immigration status, political activity or association, or other protected statuses.

Prohibited Uses:

- Conduct personal business, personal curiosity searches, or nonofficial inquiries;
- Monitor or investigate persons or groups solely because of protected activity, political viewpoint, religious practice, speech, association, or lawful exercise of constitutional rights;
- Collect information for immigration-enforcement purposes unless specifically authorized by law, Department policy, and applicable intergovernmental agreements;
- Create or maintain dossiers on individuals or groups absent a legitimate law-enforcement purpose;
- Conduct persistent or mass surveillance without a defined public-safety purpose, appropriate authorization, and legal review;
- Access, obtain, or use data through deception, pretext, false identity, or circumvention of access controls unless specifically authorized as part of an approved undercover operation;
- Use a technology output as the sole basis for an arrest, detention, search, charging recommendation, use-of-force decision, or other significant enforcement action;
- Use facial-recognition, facial-comparison, predictive, or AI-generated results as conclusive identification or probable cause without independent corroboration;
- Alter, fabricate, delete, suppress, or misrepresent technology-generated data, system logs, metadata, or investigative results;
- Share investigative information outside authorized channels or with people who do not have a lawful and operational need to know.

Documentation:

The case reports shall document:

- The system or provider used;
- The date and time of the inquiry;
- The image or data submitted;
- Results or output received;
- The corroboration performed;

If the investigative tool allows for its own internal audits, the case number and reason for the use must be documented within the investigative tool.

All suspected misuse of investigative tools will be investigated.

AJT/tlp