Policy

SEATTLE CHANNEL REMOTELY PILOTED AIRCRAFT POLICY (RPAS)

POL-303

Purpose

This policy is meant to inform and regulate the use of Remote Piloted Aircraft Systems (RPAS) by the Seattle Channel or third parties operating on behalf of the Seattle Channel.

RPAS technology acquired, even if through partnerships or contract with a third party, must still follow the provisions of all regulations and laws, including the Surveillance Ordinance, as well as adhering to the City's privacy and security requirements and this policy.

This policy will outline RPAS and its subject components, operator requirements, procedures, compliance, and other related matters.

Scope

This policy applies to the Seattle Channel's acquisition or use RPAS technologies directly or through any third party. The policy applies to usage of RPAS by Seattle Channel employees as well as by any contractors, vendors, or other third-party entities that are acting on behalf of the Seattle Channel, conducting Seattle Channel video production business.

Not in Scope:

This policy does not address:

- Regulation of RPAS by the public (e.g., hobbyists)
- Manned Aerial Systems (aircraft, helicopters, etc.)
- RPAS used for transportation or equipment delivery
- Other unmanned equipment (remotely-operated vehicles/cameras)

Policy

The Seattle Channel will follow the Federal Aviation Administration (FAA) definitions of unmanned aircraft, and any equipment associated deemed necessary for the safe and efficient operation of that aircraft. The Seattle Channel's RPAS policy is guided by best practices for RPAS use throughout the United States. It is informed by and incorporates the recommendations of public and private advocacy groups concerned with civil rights, accountability, public safety, and data minimization.

This policy will be made available to members of the public via posting to public-facing websites.

1. RPAS and Component Definition

A Remotely Piloted Aircraft (RPAS), also known as Unmanned Aircraft System (UAS), is an unmanned aircraft and the associated equipment necessary for the safe and efficient operation of that aircraft. The unmanned aircraft is one component of a RPAS. It is defined by statute as an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft (Public Law 112-95, Section 331(8)).

2. Surveillance Review

RPAS may not be acquired until completing a surveillance criteria review. If the RPAS is determined to be a surveillance technology, the request for RPAS must complete the Surveillance Impact Report process, as defined in **Ordinance 125376** including a full Council vote, prior to acquisition.

3. RPAS Equipment Privacy Controls

RPAS licensed pilots shall adhere to FAA altitude rules and not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., inside a residence or other intimate location). A Seattle Channel RPAS shall never be used for surveillance. Video or photo data shall not be used to conduct random surveillance on citizens, harass, or intimidate any individuals or group.

4. Limited Scope of Operation

Use of RPAS equipment shall be focused, limited, and controlled. Seattle Channel Operators of RPAS must have an authorized purpose to collect photos or video using a RPAS, and the use of the RPAS-collected data must meet a definitive need of the department's business. Authorization is granted by Seattle Channel Management. Personnel shall balance the use of a RPAS against other means of gathering information for a particular need and use the method that is least impactful to the public.

5. Privacy

Personnel operating an RPAS shall be mindful of privacy expectations and shall take reasonable precautions to avoid inadvertently recording or transmitting images in violation of privacy rights. Before each flight, operators should evaluate potential privacy risks such as:

- Flight paths over private property
- Unintended observation of persons
- Unintentional capture of license plates, etc.

and develop steps to mitigate those risks such as:

- Using an alternate flight route
- Not recording until over the mission area or keeping the camera angled away from potential privacy risks

Should information be incidentally collected where a person would have a reasonable expectation of privacy (e.g., inside a residence or other intimate location) that could be used to identify persons or private information, the Seattle Channel will delete the raw clip and/or remove personal identifiable information from raw data footage.

Similar to the practices and procedures in use by other governmental jurisdictions, absent a warrant or exigent circumstances, operators and observers will:

- Adhere to FAA altitude rules.
- Not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., inside a residence or other intimate location).

- Take reasonable precautions to avoid recording images in areas where there is a reasonable expectation of privacy. Reasonable precautions can include, for example, deactivating or turning imaging devices away from such areas or persons during RPAS operations.

Any raw RPAS footage retained should only be available and accessible to authorized Seattle Channel staff. All footage will be stored on a secure internal Seattle Channel server. Seattle Channel will not disclose raw, unprocessed RPAS-collected data except as required by law.

6. RPAS Operating Requirements

Pilot Licensing

For approval for FAA Certification of Authorization and/or per Title 14 of the Code of Federal Regulations (14 CFR) part 107, pilots should be FAA licensed for operations of RPAS.

Aircraft Registration

FAA regulations (14 CFR, Part 107) require that aircraft must be registered with the FAA for a fee of $5 and must be renewed every 3 years. Seattle Channel will obtain applicable authorizations, permits, or certificates required by the FAA prior to deploying or operating the RPAS. All required documentation will be maintained as required and be current.

Operating Team

Teams operating an RPAS should consist of (at-minimum): Pilot-in-Command & Visual Observer. The RPAS will be operated only by trained and FAA Certified Remote Pilots. Pilots who have reached a minimum of 50 flights and 5 flight hours will be allowed to fly solo as is allowed under FAA Part 107 rules.

Flight Planning

In the course of planning flights, employees should evaluate potential privacy risks (any routes over private property, unintended observation), and implement appropriate controls to mitigate those risks.

Flight Operations

14 CFR Part 107 mandates the following operational limitations:

- Unmanned aircraft must weigh less than 55 lbs. (25 kg).
- Visual line-of-sight (VLOS) only; the unmanned aircraft must remain within VLOS of the remote pilot in command and the person manipulating the flight controls of the small RPAS. Alternatively, the unmanned aircraft must remain within VLOS of the visual observer.
- At all times the small unmanned aircraft must remain close enough to the remote pilot in command and the person manipulating the flight controls of the small RPAS for those people to be capable of seeing the aircraft with vision unaided by any device other than corrective lenses.
- Small unmanned aircraft may not operate over any persons not directly participating in the operation, not under a covered structure, and not inside a covered stationary vehicle.

- Daylight-only operations, or civil twilight (30 minutes before official sunrise to 30 minutes after official sunset, local time) with appropriate anti-collision lighting.
- Night operations require remote pilot in command complete an updated initial knowledge test online or recurrent training, require a visual observer and the small unmanned aircraft must have lighted anti-collision lighting visible for at least three (3) statue miles that have a flash rate sufficient to avoid a collision.
- Must yield right of way to other aircraft.
- May use visual observer (VO) but not required.
- First-person view camera cannot satisfy "see-and-avoid" requirement but can be used as long as requirement is satisfied in other ways.
- Maximum groundspeed of 100 mph (87 knots).
- Maximum altitude of 400 feet above ground level (AGL) or, if higher than 400 feet AGL, remain within 400 feet of a structure.
- Minimum weather visibility of 3 miles from control station.
- Operations in Class B, C, D and E airspace are allowed with the required ATC permission.
- Operations in Class G airspace are allowed without ATC permission.
- No person may act as a remote pilot in command or VO for more than one unmanned aircraft operation at one time.
- No operations from a moving aircraft.
- No operations from a moving vehicle unless the operation is over a sparsely populated area.
- No careless or reckless operations.
- No carriage of hazardous materials.
- Requires pre-flight inspection by the remote pilot in command.
- A person may not operate a small, unmanned aircraft if he or she knows or has reason to know of any physical or mental condition that would interfere with the safe operation of a small RPAS.
- Unmanned aircraft must be equipped with Remote ID as required by FAA Remote Identification for Drone Pilots | Federal Aviation Administration (faa.gov)

Flight Logs

Seattle Channel will retain a flight log containing the date, flight time, and location of RPAS deployments. General flight information (e.g., location, date, purpose) will be made publicly available and updated quarterly through a public facing webpage or data portal.

Public Record Requirements

Data collected will be subject to the State of Washington Public Records Act (RCW 42.56).

Data Management Review

The privacy and security review includes a comprehensive data management review. Operational procedures, as well as contractual language are required to address data access, data storage, and data retention policies. Guidelines for successful operation are contained in the RPAS playbook which includes suggestions regarding departmental policies, operational policies, and legal concerns.

7. Prohibited Uses:

All RPAS acquisition or operations must involve completion of required processes including, but not limited to, a Privacy and Surveillance technology review, and if required, a Surveillance Impact Report (SIR). Use without review is prohibited.

RPAS operations shall not be used for the following:

- To conduct unauthorized surveillance activities
- To target a person based solely on individual characteristics, such as, but not limited to:
    - Race
    - Ethnicity
    - National origin
    - Religion
    - Disability
    - Gender or sexual orientation
- To harass, intimidate or discriminate against any individual or group
- To conduct personal business of any kind

Compliance

Measurement

Seattle Channel has submitted a Privacy assessment and Surveillance assessment which the Privacy Office has reviewed. Further a Security Assessment must also be conducted.

Seattle Channel will comply with all relevant FAA regulations, as well as any relevant local, state, and federal regulations.

1. Any operations determined to be subject to the Surveillance Ordinance shall be included in the annual CTO Equity Report.
2. Seattle Channel can ensure compliance with policies by maintaining complete flight logs and associated metadata and will follow standard operational procedures outlined within the RPAS Seattle Channel Flight Operations Manual (Appendix D).
3. Audits of City use of RPAS shall be conducted by the City Auditor's Office. Data should be tagged and recorded appropriately with information about the RPAS operation that will allow for greater transparency and accountability.

Exceptions

Exceptions must be approved in advance through the Seattle IT Exception Process.

Non-compliance

Enforcement of this policy will be led by the Chief Technology Officer (CTO) and may be imposed by individual division directors. Non-compliance may result in disciplinary action, restriction of access, or more severe penalties up to and including termination of employment or vendor contract.

Related Standards and Policies

- Public Law 112-95, Section 331(8) – Defines RPAS
- SMC 14.18 - requires that RPAS undergo a privacy and surveillance review as defined in Ordinance 125376
- Title 14 of the Code of Federal Regulations (14 CFR) part 107 – RPAS operational requirements
- FAA SEC. 334. Public Unmanned Aircraft Systems – mandate RPAS teams minimum
- RCW 42.56 – State of Washington Public Records
- Information Technology Security Policy

Responsibilities

The Privacy Office is the only group that may officially determine whether a technology (hardware or software) is a surveillance technology. The Chief Technology Officer ultimately is responsible for this determination and is accountable to both the Executive and City Council for reporting surveillance technology acquisitions. Due to sensitive privacy and civil liberties considerations, the Privacy Office will work with Compliance to coordinate stakeholder engagement.

Contacts

Subject	Role	Name/Title	Email
		Shannon Gee/General Manager	Shannon.Gee@seattle.gov
		Ed Escalona/Production Manager	Ed.Escalona@seattle.gov
		Peter Cassam/VS II RPAS Team lead	Peter.Cassam@seattle.gov

Definitions

Remotely Piloted Aircraft Systems (RPAS): also referred to as drones, unmanned aerial aircraft, or unmanned aerial vehicles, are aerial equipment used to gather information from an airborne perspective that is operated remotely and without direct human interaction from within or on the aircraft.

- Most systems use a camera or recording device to capture or transmit data from an aerial perspective
- May also be equipped with additional sensing technologies such as infrared or Lidar (Light Detection and Ranging) and,

- May have differing capabilities of recording videos or photos for storage or real time transmission
- The equipment used on a system may vary by the intended use and objective of the RPAS

Authority

This policy is governed by the City of Seattle Surveillance Ordinance, City of Seattle Privacy Policy and Privacy Principles, as well as the City's security and compliance requirements. This policy does not replace any existing policies regarding security or compliance and should only complement them.

Document Control

8. Effective Date

This policy shall be effective on 7/1/2023.

9. Review Cycle

This policy shall be reviewed annually. The next review shall occur by July 1 2024.

Version	Content	Contributors	Approval Date
v 1.0	Initial Draft	Contributors: 1. Peter Cassam, Shannon Gee – Seattle Channel 2. Sarah Carrier, Eleonor Bounds – Privacy 3. Keith Cooke – Compliance Reviewers: 4. Ginger Armbruster – ITD DPAC 5. Greg Smith - CISO	
	Final	**Approver:** **Jim Loter - Chief Technology Officer (Interim)**	**6/30.2023**

Appendix B: Glossary & Definitions

CJIS: "Criminal Justice Information Systems"

FAA: "Federal Aviation Administration"

ITD: "Seattle Information Technology Department"

LiDAR: "Light Detection and Ranging"

PIC: "Pilot in Command"

RPAS: "Remotely Piloted Aircraft"

SCL: "Seattle City Light"

SDOT: "Seattle Department of Transportation"

SFD: "Seattle Fire Department"

SIR: "Surveillance Impact Report

SPD: "Seattle Police Department"

UA: "Unmanned Aircraft"

UAS: "Unmanned Aerial System"

sRPAS: "Small Unmanned Aerial System"

VLOS: "Visual Line of Sight"

VO: "Visual Observer"

For more information on FAA guidelines and regulated airspace, please see the following manual: https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/phak/media/17_phak_ch15.pdf

Appendix C: Surveillance Checklist

Does the technology meet the following definition?

- Technology whose primary purpose is to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals whose identity can be revealed by license plate data when combined with any other record.

Do any of the following exclusion criteria apply?

- Technology that is used to collect data where an individual knowingly and voluntarily provides the data.
- Technology that is used to collect data where individuals were presented with a clear and conspicuous opt-out notice.
- Technologies used for everyday office use.
- Body-worn cameras.
- Cameras installed in or on a police vehicle.
- Cameras installed pursuant to state law authorization in or on any vehicle or along a public right-of-way solely to record traffic violations.
- Cameras installed on City property solely for security purposes.
- Cameras installed solely to protect the physical integrity of City infrastructure, such as Seattle Public Utilities reservoirs.
- Technology that monitors only City employees in the performance of their City functions.

Do any of the inclusion criteria apply?

- The technology disparately impacts disadvantaged groups.
- There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.
- The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.
- The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

To require a Surveillance Impact Review and inclusion on the Master List, the technology in question must **meet the definition of surveillance**, have **no** exclusion criteria and at least **one** inclusion criteria.

Appendix D: Additional Resources

The following external resources may be useful as departments consider best practices and special considerations for RPAS use involving critical infrastructure:

- FAA: Operate a Drone, Start a Drone Program
- Voluntary Best Practices for RPAS Privacy, Transparency, and Accountability
- Department of Homeland Security - RPAS
- IAFC RPAS Toolkit
- ICAO RPAS Toolkit
- Third Party Hostile Takeovers of Unmanned Aircraft: Law, Policy, and Implications for Business
- CISA Best Practices
- ACLU Guidance
- 2021 Executive Order
- FAA Advisory Circular
- RPAS Seattle Channel Flight Operations Manual (FOM)

1.1.1.