Policy for the Collection, Handling, Release and Privacy of Data and Images Acquired Through ODOT Unmanned Aircraft Systems Vehicles

POLICY STATEMENT:

The Ohio Department of Transportation (ODOT) has an obligation to protect one’s privacy while maintaining full transparency, as required under Ohio’s Public Records Laws. This policy governs the images and data collected from Unmanned Aircraft Systems Vehicles (UAS). ODOT intends to make this data available while recognizing individuals’ privacy.

Although the courts have held that there is no reasonable expectation of privacy with respect to aerial surveillance because of the ability that anyone might have to observe what could be viewed from the air, this policy provides the requirements for protecting the privacy of people who have images and information about them inadvertently gathered through ODOT’s data acquisition systems.

SCOPE:

This Policy applies to all employees, collaborators and contractors of ODOT and shall govern their collection and handling of data and images from UAS vehicles and their responding to public record requests for this data from any public or private entity.

BACKGROUND AND PURPOSE:

For many years, ODOT has acquired aerial photographic data, data from roadway cameras, and data from hand held devices to plan, design and build Ohio’s roadways and bridges. With the development of modern technology, these devices, including but not limited to UAS mounted cameras, are able to acquire images of land, buildings, and other structures more precisely and more conveniently than ever before. ODOT has legitimate business purposes for seeking these images and data in the areas such as mapping, construction and bridge inspections.

Given the myriad of uses of the data and photo-imagery ODOT may acquire, it is necessary to create a policy that will allow the collection, retention and access to this data while also maintaining the privacy of those images or other information inadvertently acquired.
TRAINING:

ODOT employees and contractors who gather data by means of UAS vehicles will have appropriate training consistent with this Policy. ODOT employees who deal with the data collected and with public records requests and inquiries will also receive training as to this Policy.

The distribution of this policy along with subsequent guidelines, and procedures will constitute training on this policy. Questions regarding this Policy should be directed to ODOT’s Division of Chief Legal Counsel.

FISCAL ANALYSIS:

Compliance with this Policy will require minor additional staff time and no additional purchase of equipment so the fiscal impact to ODOT will be minimal.

DEFINITIONS:

UAV/UAS: Unmanned aerial vehicles (UAVs), are aircraft that can fly without an onboard human operator. An unmanned aircraft system (UAS) is the entire system, including the aircraft, digital network, and personnel on the ground.

Data: Any information that ODOT employees or contractors obtain via UAS vehicles being flown for ODOT purposes. Data includes, but is not limited to audio recordings, visual images or any collected material and analyses thereof. Data, for purposes of this policy, does not include any information obtained by any other public or private entity or individual leasing and using any ODOT owned UAV/UAS. Any data collected or obtained by any other entity or individual is the property of that entity or individual and not the property of ODOT and; therefore, is outside the scope of this policy.

UAV/UAS Pilot: A person exercising control over a UAV/UAS during flight.
PROCEDURE:

1. Data collection

During a UAS flight, if it is apparent that data beyond the scope of the purpose of the flight will be obtained or collected, the collection of data should be suspended if possible until the non-relevant images or information are no longer within the collection field of the UAV.

Any data that is inadvertently collected and is beyond the purpose of the UAS flight, should, if possible, be immediately deleted upon discovery.

If any data is inadvertently collected but cannot be deleted due to the existence of relevant data, the inadvertent data should be obscured beyond recognition if at all possible.


Data is subject to the Ohio Public Records Laws pursuant to Ohio Revised Code Chapter 149.

3. Data and Image Retention

ODOT will follow the Ohio Department of Administrative Services’ records retention schedule for retaining data. Specifically for Photo Files, GAR-RPM-05 and Audiovisual Materials GAR-RPM-06, data will be retained until information is no longer current then transferred to State Archives for possible retention or destruction.

5. Requests for Data

Any requests for Data shall be handled pursuant to ODOT’s Procedure for the Handling of Public Record Requests – Standard Procedure 150-001(SP) dated November 18, 2015.

4. Requests for Inadvertent Data

Any requests for inadvertent data by law enforcement or others shall be referred to ODOT’s Division of Chief Legal Counsel.
STANDARD PROCEDURE

All personnel shall follow the below requirements and procedures when handling personal or sensitive information or information that could reasonably be construed as personal or sensitive.

a. Take reasonable precautions to not collect any data that does not pertain to the purpose of the UAS flight.
b. Review all data after a flight to ensure that any inadvertent information was not collected.
c. Take reasonable precautions to ensure the secure and complete destruction of any inadvertent data.
d. Keep the data for only as long as is required by the records retention schedule unless otherwise instructed due to a valid request for this data having been received.
e. Whenever a request for data is received, follow all ODOT public record policies and review all data prior to disclosure to ensure that no inadvertently collected information will be disclosed.

Employees always have a duty not to disclose data inadvertently collected beyond the purpose of the flight without proper authorization. If you suspect such data has been improperly accessed or disclosed, you shall report the incident to your supervisor or contact the Division of Chief Legal Counsel.

VIOLATIONS

Any employee who violates this policy is subject to disciplinary action up to and including termination and a lifelong prohibition against working for the State of Ohio. The employee may also be subject to criminal charges and/or civil liability arising out of the employee’s actions. An employee who complies in good faith with this policy is not subject to discipline under this policy.

Any violation of this policy by a collaborator or contractor may be considered a material breach of the agreement or contract and may subject the agreement or contract to termination. If the violator is a vendor, s/he may also be subject to vendor debarment. Any collaborator or contractor who violates a confidentiality statute may also be subject to criminal charges and/or civil liability arising out of the collaborator’s or contractor’s actions.