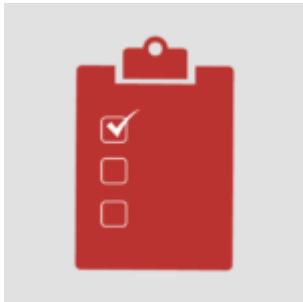


OHS-Related Drones Systems Use Compliance Checklist



Increasing numbers of companies are using remotely piloted aircraft systems (RPAS), aka drones, to carry out occupational health and safety (OHS) program functions. One prominent application is using drones embedded with video cameras, GPS, sensors, communication equipment and artificial intelligence (AI) algorithms that fly over a work site and relay real-time information to perform aerial inspections and monitoring to ensure that all required safety measures and procedures are being properly implemented. Using drones instead of workers to inspect equipment or conditions in elevated surfaces or spaces may also be an effective way to minimize vertical fall hazards.

As with most forms of AI technology, using drones to conduct inspections, monitoring, or other workplace safety activities can get you into trouble under privacy laws. The problem is that the data drone systems capture, analyze, and store may include images and other personal information about workers, visitors, and members of the public that's protected by privacy laws.

Because this is such a novel issue, it's easy for OHS directors to overlook. Even if you are tuned in to the privacy implications of drones use, it's hard to find guidance or best practices you can rely on. The good news is that the Ontario Information and Privacy Commission (OIPC) just published cutting edge guidance on responsible use of drones systems.

Although directed at police and law enforcement, much of the OIPC would apply to using drones to monitor, inspect, and ensure a safe workplace.

Here's a Checklist of recommended measures you can use if you currently or are thinking about deploying drones at your own workplace.

Drones System Compliance Review Checklist

Site/Facility: _____

Building/Area/Work Zone: _____

Date of Review: _____ **Time:** _____

Reviewer Name & Title: _____

1. Lawful Authority & Operation

Before implementing a program involving the use of drones for workplace health and safety purposes:

- ☐ Ensure you have lawful authority to operate drones for those workplace health and safety purposes
- ☐ Ensure that authority is clearly documented
- ☐ Ensure the design and operation of the drones program meets all applicable legal requirements
- ☐ In the case of existing drone programs, if there are any gaps or uncertainty regarding compliance or legal authority, temporarily halt the program and make the necessary adjustments to bring it into compliance before resuming operation

2. Drones System Guiding Principles & Statement of Purpose

- ☐ Develop and communicate to affected workers a statement of guiding principles for the use of drones that addresses issues of privacy, transparency, and accountability
- ☐ Comply with these principles throughout all stages of

design, deployment, and operation of the drones program

- Clearly define the scope, limits, and purpose of your drones program
- Verify that use of drones is reasonable, necessary, and proportionate for that scope and purpose
- Verify that anticipated health and safety benefits outweigh potential risks to privacy and other fundamental rights
- Identify situations where drones may not be used
- After making changes to your drones program, adjust its scope and purpose, and reverify that it complies with applicable laws and privacy principles
- Identify any unique capabilities of your drones system
- Assess how those system-specific drones features will be used, or restricted, in specific operational contexts

3. Drones System Privacy Impact Assessment

- Conduct a comprehensive Privacy Impact Assessment (PIA) before deploying a drones program
- Consider whether the specific problems the drones program addresses are necessary and substantial
- Consider whether there are less intrusive alternatives available for resolving those problems
- Consider the surveillance capabilities of the drone to collect, use, retain, and/or disclose personal information protected by privacy laws
- Assess the risk that the drone will capture personal information about workers or other people who are not the target of or involved in the problems the drones system is being used to resolve

- Consider whether drones will be deployed in and around private spaces, such as a residential area
- Determine the maximum length of time a drone will monitor a target and whether the drone will follow a target moving between different locations
- Identify appropriate safeguards to prevent or limit capturing personal information incidentally or indirectly
- Share the results of the PIA with the workplace joint health and safety committee, health and safety representative, the affected workers, and the workers' union
- Update the PIA if there is a significant change to the purpose for which the personal information is collected, used, or disclosed, or other significant change to an existing drones program

4. Drones Program Policies & Procedures

- Create, in consultation with the workplace joint health and safety committee, health and safety representative, the affected workers, and the workers' union, comprehensive policies and procedures for the drones program
- Ensure that your drones policies and procedures are consistent with the scope and purpose of the program listed in accordance with Section 2 above
- Review and update your drones policies and procedures on a regular basis and whenever substantial changes are made to the program to ensure continued alignment with legal requirements, operational realities, and evolving best practices
- Ensure that program policies and procedures are readily accessible to all affected workers and their representatives
- Include a glossary of key terms and definitions specific to your drones system to ensure consistent understanding of

technical, operational, and procedural requirements across all personnel

5. Limitations on Collection, Use, Disclosure, & Retention of Personal Information

- Ensure that the collection, use, disclosure, and retention of personal information by your drones system is limited to what is necessary and proportionate for achieving a legitimate health and safety purpose
- Ensure that privacy protective policies are in place and that specifically address company use of drones near private or sensitive spaces such as residences, religious or spiritual places, or healthcare settings
- Ensure that the requirements for the collection, use, disclosure, retention, and secure destruction of personal information are established in compliance with relevant laws, regulations, policies, or procedures

6. Physical Controls & Safeguards

- Implement technical, administrative, and physical controls and safeguards for the collection, use, disclosure, and retention of personal information captured by drones, which may include:
 - Use of geofencing
 - Flight path restrictions
 - Masking or blurring technologies
 - Encryption and access controls
 - Secure transmission Anti-interception technologies
 - Incident response procedures

7. Transparency

- Provide written, visual, auditory and/or verbal notices to

inform workers, visitors, and, if necessary, the public of when and where a drone is deployed

- Provide up-to-date, readily available and plain-language information about your drones program

8. Accountability

- Implement a robust governance regime to ensure accountable and transparent use of drones and drones-generated data by company personnel
- Implement policies, practices, physical barriers, and technological controls to protect drone-generated records against theft, loss, unauthorized access, use, disclosure, modification, or destruction
- Conduct scheduled drone systems audits to ensure compliance with all applicable laws, policies, procedures, and standards
- Regularly report drones system data audit findings to stakeholders
- Reassess and update drones policies, procedures, and protections that are found to be insufficient and bring them into alignment with privacy requirements and best practices

9. Drones Systems Training

- Ensure operators have the technical competence, policy knowledge, and legal understanding required to safely and effectively conduct drones operations
- Establish a training program that covers the unique characteristics of the drone systems to be deployed and how to mitigate privacy risks associated with the drones' capabilities
- Ensure operators understand their responsibility for ensuring that all drone uses comply with legal requirements,

respect an individual's reasonable expectation of privacy, and avoid unnecessary or disproportionate intrusions

- Regularly review and update the content of training programs to reflect new legal or policy requirements, evolving technical capabilities, and emerging risks identified through pilot programs, audits, PIAs, and other related risk assessments
- Ensure that all drones systems remain under meaningful human control at all times

10. Access to & Correction of Personal Information

- Implement a process for responding to individual workers' requests for access and correction of their personal information
- Give workers plain language information on how they can access and correct their personal information captured by drones
- Ensure such information is readily available to workers

11. Drone Program Monitoring & Reassessment

- Continuously monitor your use of drones
- Conduct regular reviews of your drones programs, policies, and procedures to identify emerging or evolving risks, including technical risks, changes in legal or regulatory requirements, and unintended consequences arising from operational use
- Where necessary, take appropriate corrective action to update policies and procedures, operational controls, technical safeguards, operator training, PIAs and related assessments
- As part of the reassessment process, evaluate whether the

drones program continues to meet its intended objectives and whether its use remains necessary, effective, and proportionate to the problems it's designed to address—and cease, limit, or adjust the program in accordance with the findings

- Maintain detailed logs to record when drones data containing personal information is disclosed or transferred, recording by whom and for what purpose, and any subsequent access, modification, dissemination or deletion of data, where and as appropriate.

You can download this checklist in doc and PDF formats below.