

Homeowners Association Technology, Privacy, and Surveillance Guidelines

Proposed Policy for Adoption by the Homeowners Association

Effective Date: _____

Adopted By: _____

HOA: _____

1. Purpose and Policy Statement

The purpose of these guidelines is to protect residents' reasonable expectations of privacy, safety, quiet enjoyment of their property, and freedom from unreasonable technological surveillance or interference while recognizing the legitimate use of technology for security, safety, communication, and community purposes.

Technology changes rapidly. Accordingly, these guidelines apply not only to the specific devices identified below but also to substantially similar technologies developed or introduced after adoption of these guidelines.

Nothing in these guidelines is intended to prohibit technology that is otherwise lawful and does not unreasonably interfere with another resident's privacy, safety, property rights, or quiet enjoyment of his or her home.

2. Video Cameras and Video Surveillance

A. General Privacy Rule

Residents may install security cameras on their property for legitimate purposes such as protecting their home, family, vehicles, packages, and personal property.

A camera may not be positioned or operated for the primary purpose of monitoring, surveilling, following, or recording another resident or that resident's private activities.

A resident shall not aim a camera directly into another resident's backyard or other private outdoor area when there is a reasonable expectation of privacy.

A reasonable expectation of privacy may be demonstrated by circumstances including, but not limited to:

- A privacy fence;
- Landscaping, trees, shrubs, or other natural screening;
- Privacy screens or other barriers;
- A structure or enclosure intended to prevent observation;
- Other reasonable measures taken by the resident to shield the area from view.

The existence of a fence, landscaping, or other privacy measure does not automatically make an area legally private; however, it shall be considered by the HOA when determining whether a camera's placement constitutes unreasonable surveillance. No Wifi enabled video surveillance cameras may capture another resident's home.

B. Front and Side of Neighboring Homes

A Wi-Fi-enabled, internet-connected, cloud-connected, or remotely accessible camera shall not be intentionally aimed directly at another resident's front-facing living area, side of house, windows, doors, patio, porch, or other area where the positioning creates an unreasonable opportunity to monitor the resident or household.

A camera intended to monitor a resident's own driveway, entrance, sidewalk, or property should be positioned and configured to minimize capture of a neighboring property.

Where technically possible, privacy masking, privacy zones, camera angle adjustments, or similar manufacturer-provided features shall be used.

C. Camera Mounting Height

No residential video surveillance camera may be mounted higher than **eight (8) feet above ground level** without prior written approval from the HOA Board.

The HOA may approve a higher mounting location when reasonably necessary for security, safety, property protection, or another legitimate purpose and when the installation does not create an unreasonable privacy intrusion.

This height limitation applies to the camera and its mounting hardware, not necessarily to the structure on which the camera is attached.

D. Second-Level Windows

No camera may intentionally capture, monitor, or be positioned to directly view the second-level windows of another resident's home.

Where technologically possible, privacy masking or other camera configuration shall be used to exclude neighboring second-level windows from the recording area.

HOA can require to see video footage of any camera that violates these intentions.

E. Camera Complaints and HOA Review

All complaints concerning alleged improper camera placement, recording, surveillance, or privacy violations shall be submitted to the HOA Board in writing.

The Board shall:

1. Acknowledge the complaint immediately;
2. Review the relevant facts within 3 days;

3. Provide the camera owner an opportunity to respond withing 5 days;
4. Review photographs, diagrams, camera positioning, and other relevant information within 2 days;
5. Where reasonably necessary, request the camera's make, model, specifications, field of view, mounting height, recording capabilities, storage method, and relevant configuration information;
6. Where reasonably necessary and legally permissible, request representative video footage or screenshots sufficient to determine what the camera captures; and
7. Render a written decision within seven (7) calendar days after receiving sufficient information to evaluate the complaint.

The seven-day period may be extended when the Board reasonably determines that additional information, inspection, legal advice, or technical evaluation is necessary. The Board should notify the parties when an extension is required.

The HOA shall not require disclosure of unrelated personal recordings or private information beyond what is reasonably necessary to resolve the complaint.

F. Audio Recording

Because audio recording may raise additional privacy concerns, cameras should have audio recording disabled when audio is not necessary for the legitimate security purpose of the camera.

Residents shall not intentionally use a camera's microphone to monitor or record private conversations occurring on another resident's property.

Audio recordings are a violation of federal laws.

G. Recording and Retention

Video recordings should be retained only for a reasonable period necessary for the legitimate purpose for which they were collected.

Residents should not maintain recordings of neighbors indefinitely for the purpose of monitoring their activities.

Recordings shall not be publicly distributed, posted to social media, transmitted to other residents, or otherwise shared for the purpose of harassment, embarrassment, intimidation, or retaliation.

Nothing in this provision prevents a resident from providing relevant footage for legal purposes.

H. Facial Recognition and Automated Surveillance

A resident shall not use facial-recognition technology, automated person tracking, license-plate recognition, or similar technology primarily to monitor another resident's movements or activities.

Technology used for legitimate security purposes shall be configured, where reasonably possible, to minimize collection of information concerning neighboring residents.

I. Temporary Cameras

Temporary cameras, trail cameras, wildlife cameras, game cameras, or similar devices are subject to the same privacy requirements as permanently installed cameras.

A resident may not use a temporary camera as a means of circumventing these guidelines.

J. HOA Inspections

When the HOA receives a credible complaint, the Board may request reasonable information regarding the camera's location, mounting height, field of view, technical specifications, and privacy settings.

The HOA shall not enter a resident's home or property to inspect equipment without the resident's permission, legal authority, or another lawful basis.

K. Prohibited Uses

Technology shall not be used to:

- Harass, threaten, intimidate, or retaliate against another resident;
- Follow or track a resident's movements;
- Monitor a neighbor's visitors or guests for non-security purposes;
- Record private activities occurring in a protected area;
- Create a dossier or surveillance history of another resident;
- Publish private recordings for purposes of humiliation or retaliation; or
- Circumvent another resident's reasonable privacy measures.
- Monitor a neighbor for other parties.

3. Electronic and Electric Fences

A. HOA Approval Required

No electronic, electric, invisible, underground, radio-frequency, or similar fence system may be installed without prior written approval from the HOA Board.

Where the proposed installation may affect an adjoining property, the applicant must also obtain written consent from the affected neighboring resident(s).

B. Types of Systems

These provisions include, but are not limited to:

- Electric fences;
- Electrified barriers;

- Invisible dog fences;
- Underground pet containment systems;
- Radio-frequency boundary systems;
- GPS-based property boundary systems;
- Electronic gates and barriers; and
- Similar systems that create a physical, electrical, radio, or technological boundary.

C. Safety

No system may:

- Create an unreasonable risk of injury;
- Interfere with emergency access;
- Interfere with utility equipment;
- Create unreasonable interference with neighboring electronic equipment;
- Be installed in a common area without HOA authorization; or
- Violate applicable building, electrical, zoning, fire, or safety requirements.

D. Neighboring Properties

An electronic boundary may not be programmed or installed so that it extends onto or materially affects another resident's property without that resident's written consent and HOA approval.

E. Maintenance

The property owner is responsible for maintaining the system in a safe condition and promptly correcting malfunctioning equipment.

The HOA may require removal or modification of an electronic fence that creates a demonstrated safety hazard or violates these guidelines.

4. Drone and Unmanned Aircraft Technology

A. General Rule

Residents may not operate drones that invade another resident's airspace or privacy. HOA encourages usage for lawful recreational, personal, or commercial purposes provided the operation is outside of the community.

Current technology has made it possible to utilize drones in a variety of shapes: Bumble bee, dragon fly, birds, and other inconspicuous forms. These drones are forbidden by the HOA.

A resident who believes a drone is invading privacy, creating a safety hazard, trespassing, or otherwise violating the law should document the incident from a safe location and contact the HOA and, where appropriate, law enforcement or the applicable aviation authorities

B. Prohibition on Surveillance of Residents

No resident may intentionally use a drone to monitor, follow, surveil, photograph, or record another resident or the interior of another resident's home without appropriate authorization or consent.

Particular care shall be taken regarding:

- Bedrooms;
- Bathrooms;
- Second-story windows;
- Enclosed patios;
- Private backyards;
- Swimming pools;
- Areas enclosed by privacy fences;
- Areas shielded by landscaping; and
- Other areas where there is a reasonable expectation of privacy.

The HOA may treat repeated drone activity directed at a particular resident or property as potential harassment or an unreasonable privacy intrusion.

C. No Hovering for Surveillance

A drone shall not hover outside or over a resident's property for the purpose of observing or recording the resident, family members, guests, or private activities.

Normal transit through lawful airspace is distinguishable from targeted surveillance.

D. Drone Registration and Compliance

Where required by law, drone operators are responsible for registration, Remote ID, airspace authorization, pilot requirements, and other applicable requirements.

5. Frequency Monitoring, Signal Jamming, and Radio-Frequency Equipment

A. Prohibition on Jamming

No resident may operate, deploy, install, or intentionally use a radio-frequency jammer, cell-phone jammer, GPS jammer, Wi-Fi jammer, Bluetooth jammer, drone jammer, or similar device to interfere with communications or electronic signals.

Federal law prohibits the operation, marketing, sale, and importation of signal jammers in the United States, including on private property.

B. Targeted Interference

A resident shall not intentionally interfere with another resident's:

- Cellular service;
- Wi-Fi;
- Bluetooth;
- GPS/GNSS;
- Radio communications;
- Wireless security equipment;
- Garage-door communications;
- Smart-home systems; or
- Other lawful communications.

C. Frequency Monitoring

Passive use of ordinary, lawful radio-frequency monitoring equipment for legitimate purposes is not automatically prohibited. However, no resident may use monitoring equipment as part of a program to surveil, harass, stalk, interfere with, or collect private information concerning another resident.

Any equipment capable of transmitting, disrupting, intercepting, or modifying communications must comply with all applicable federal laws and regulations.

D. Suspected Interference

Residents who believe that their communications or electronic equipment are being intentionally interfered with should document the problem and report it to the HOA.

The HOA may refer suspected unlawful radio-frequency interference to the appropriate governmental authority.

6. Motion Detectors

A. General Use

Residents may not aim a motion detector to capture another resident's motion on their private property.

Technology shall not be used to harass, threaten, stalk, intimidate, or invade the privacy of another resident.

A resident who believes motion detector are being used to monitor their property should contact the HOA and, where appropriate, law enforcement.

B. Recording Other Residents

Residents should not intentionally photograph, video-record, or audio-record another resident in a location where that person has a reasonable expectation of privacy.

Particular care shall be taken when recording:

- Inside another person's home;
- Through windows;
- Behind privacy fences;
- In bathrooms or changing areas;
- In bedrooms;
- In private backyards; or
- During private conversations.

Applicable state and federal recording laws must be followed.

C. Location Tracking

Residents may not intentionally place a GPS tracker, Bluetooth tracker, AirTag-type device, or similar tracking device on another person's vehicle, bicycle, personal property, or belongings without authorization.

This prohibition does not prevent lawful tracking of one's own property or devices.

D. Harassing Communications

Electronic communications, including text messages, email, social-media messages, and other digital communications, shall not be used to threaten, stalk, intimidate, or harass another resident.

Disagreements between residents should be addressed through the HOA's established dispute-resolution process rather than through electronic harassment.

7. Smart Doorbells and Smart-Home Devices

Smart doorbells, security systems, smart speakers, microphones, and other connected devices are permitted when used responsibly.

Residents should configure these devices to minimize unnecessary capture of:

- Neighboring homes;
- Neighboring yards;

- Private conversations;
- Windows;
- Neighboring doorways; and
- Other private areas.

Smart devices shall not be deliberately positioned to monitor a neighboring resident's daily activities.

8. Hidden Cameras and Covert Surveillance

The use of hidden cameras, concealed recording devices, disguised microphones, or other covert surveillance equipment to monitor another resident's private activities is prohibited.

This provision does not prohibit legitimate security devices that are reasonably visible or that are installed for the protection of the resident's own property.

9. Artificial Intelligence and Automated Surveillance

Residents shall not use artificial intelligence or automated technology to create or maintain surveillance of another resident.

Examples include:

- Facial-recognition systems;
- Automated person identification;
- Automated license-plate tracking;
- AI-based behavioral monitoring;
- Voice identification;
- Automated movement tracking;
- Predictive tracking of a resident's activities; and
- Similar technologies.

Legitimate security applications may be permitted when they are reasonably limited in scope and do not create an unreasonable privacy intrusion.

10. Laser, Infrared, and Other Optical Technology

No resident may intentionally direct lasers, high-powered lights, infrared illuminators, thermal imaging devices, or similar optical equipment toward another resident's home for the purpose of monitoring, disturbing, intimidating, or interfering with the resident.

Security lighting and ordinary exterior lighting are permitted when reasonably designed to illuminate the owner's property without creating an unreasonable nuisance or privacy intrusion.

11. Cybersecurity and Network Interference

No resident may intentionally:

- Access another resident's Wi-Fi network without authorization;
- Attempt to obtain another resident's passwords;
- Hack another resident's smart-home devices;
- Access another resident's security cameras;
- Disable another resident's electronic security equipment;
- Intercept another resident's private electronic communications; or
- Deliberately disrupt another resident's internet or network service.

Residents should secure their own networks using reasonable security practices.

12. Technology Used for Harassment or Retaliation

Regardless of the specific technology involved, no device or technology may be used for the purpose of:

- Harassment;
- Stalking;
- Intimidation;
- Retaliation;
- Threatening behavior;
- Surveillance;
- Coercion;
- Deliberate interference;
- Embarrassment; or
- Creating an unreasonable disturbance to another resident.

The fact that a device is commercially available or technologically capable of performing an activity does not make that activity permissible under these guidelines.

13. Technology Complaints

A resident who believes these guidelines have been violated should submit a written complaint to the HOA Board.

To the extent reasonably available, the complaint should include:

- Date and approximate time;

- Location;
- Description of the device;
- Description of the alleged activity;
- Photographs or video evidence, if lawfully obtained;
- Names of witnesses, if any; and
- A description of the impact on the complaining resident.

The HOA shall handle complaints in a fair and consistent manner.

The Board may request reasonable technical information from the alleged violator when necessary to determine whether the technology complies with these guidelines.

The HOA shall avoid requesting or retaining unrelated private information.

14. Investigation and Enforcement

Upon receiving a complaint, the HOA Board may:

1. Review the complaint;
2. Request information from the parties;
3. Request photographs, diagrams, specifications, or relevant recordings;
4. Conduct a reasonable exterior inspection where permitted;
5. Consult technical experts or legal counsel;
6. Determine whether the HOA's governing documents or these guidelines have been violated;
7. Require reasonable corrective action; and
8. Apply remedies authorized by the HOA's governing documents and applicable law.

The HOA shall apply these provisions consistently and without discrimination.

15. Evidence and Privacy

When a resident provides video, photographs, recordings, or electronic evidence to the HOA, the HOA shall use the material only for legitimate purposes related to the complaint, enforcement, safety, or legal obligations.

The HOA should limit distribution of such material to Board members, management, legal counsel, insurers, investigators, persons with a legitimate legal cause, or other persons with a legitimate need to review it.

16. Changes in Technology

Because technology develops rapidly, these guidelines shall be interpreted to apply to substantially similar technologies even when a particular device or technology is not specifically named.

The Board may propose amendments as new technologies become commonly available.

Any amendment shall be adopted in accordance with the HOA's governing documents and applicable law.

17. Severability

If any provision of these guidelines is determined to be invalid, unlawful, or unenforceable, the remaining provisions shall remain in effect to the fullest extent permitted by law.

18. No Waiver of Legal Rights

These guidelines are intended to supplement, and not replace, applicable law and the HOA's governing documents.

Nothing in these guidelines creates a right to engage in conduct that is otherwise unlawful, nor does adoption of these guidelines eliminate any legal rights or remedies available to a resident, the HOA, or another person under applicable law.

19. Recommended Board Review

Before adoption, the HOA Board should have its attorney review these guidelines specifically for:

- State privacy and recording laws;
- HOA authority under the governing documents;
- Property and trespass laws;
- Drone and unmanned-aircraft regulations;
- Federal communications laws;
- Applicable municipal ordinances;
- Disability/accessibility requirements;
- Fair-housing requirements;
- Enforcement and fine procedures; and
- Due-process requirements for HOA violations.

Proposed by: _____

Date: _____

Board Approval: _____

Effective Date: _____