

PROTECTING THE PRIVATE SPHERE



Electronic Safety & Public Records Primer

A Civic Guide for Newly Elected Officials on
Personal Communications, Compliance & Family Protection
under Florida Law.

PROTECTING THE PRIVATE SPHERE

Electronic Safety & Public Records Primer

A Civic Guide for Newly Elected Officials on Personal Communications, Compliance & Family Protection under Florida Law

IMPORTANT DISCLAIMER: This document is for general informational and educational purposes only. It is not legal advice and does not create an attorney-client relationship. Florida public records law (Chapter 119), the Government in the Sunshine Law (Chapter 286), and related statutes are fact-specific. Destruction of public records is a criminal offense. Newly elected officials should consult their municipal or county attorney and, if desired, private counsel experienced in Florida open-government law before adopting any practices described here.

1. Purpose of This Primer

Serving in elected office brings heightened public scrutiny, increased volume of public records requests, and elevated risks of personal and family targeting—especially during controversial periods. This primer provides newly elected candidates and officeholders with a practical, full-spectrum framework for:

- Keeping purely personal communications with family, friends, and non-official team members outside the scope of Florida’s public records law.
- Maintaining strict compliance when official business is discussed.
- Reducing the digital and public footprint that can expose immediate and extended family to harassment or doxxing.

The recommendations emphasize proactive segregation of devices, accounts, and habits rather than reactive workarounds.

2. Core Legal Framework (Florida)

Public Records – Content Is Decisive

Under Chapter 119, Florida Statutes, a public record is any material made or received in connection with the transaction of official business that is intended to perpetuate, communicate, or formalize knowledge. The form (email, text, Signal message, social media direct message, note) and the location (government device, personal phone, private email account) do not control. Content and purpose do.

- **Purely personal communications** — family logistics, pure social conversation, or pure political/campaign strategy that does not discuss official agency business — are generally not public records, even if they occur on a government device or account. (See *State v. City of Clearwater*; *Butler v. City of Hallandale Beach*.)
- **Official business on personal devices/accounts** — any discussion of agency business, agendas, staff matters, development issues, or constituent concerns in an official capacity creates a public record. The agency has a duty to retrieve it. (See *O’Boyle v. Town of Gulf Stream*; *City of Sunny Isles Beach v. Gatto*.)
- **Encryption is not an exemption.** If content qualifies as a public record, it must still be retained and produced. Deleting or destroying potential public records can constitute a crime.

Sunshine Law

Chapter 286 prohibits discussions among two or more members of a collegial body about matters that may foreseeably come before the body, unless the discussion occurs in a properly noticed public meeting. This applies to electronic communications (email, text, group chats, social media).

Recent Privacy Protections for Officials and Families

As of July 1, 2025, Florida law expanded exemptions (SB 268 and related provisions) for certain identifying and location information of city and county commissioners (and other public officers), their spouses, and adult children. This commonly includes home addresses (with partial-address nuances), personal telephone numbers, and related details for minor children (school/daycare names and locations). Officials should promptly file written exemption requests with the relevant agencies (municipality/county, property appraiser, supervisor of elections, and others holding the data).

3. Recommended Full-Spectrum Electronic Pattern

The objective is bright-line technical and behavioral separation so that pure personal communications remain personal, official business stays on official channels (and is properly retained), and family digital exposure is minimized.

3.1 Device and Account Architecture

- **Prefer two physical devices.** One dedicated to official use (government-issued if available, or a secondary phone used exclusively for official accounts). The primary personal phone should never log into official accounts and should not store official contacts or calendars.
- **If one device is unavoidable:** Use dual-SIM/eSIM with strict separation, or OS-level work profiles / secondary user profiles. Never share the same Apple ID or Google account across official and personal contexts.
- **Email separation:** Official government account exclusively for duties. Personal account(s) strictly for non-official use. Privacy-oriented personal email providers are reasonable for sensitive personal correspondence.
- **Contacts and calendars:** Completely separate lists. Family and pure personal contacts live only on the personal side.
- **Social media:** Strictly separate accounts. Official accounts should be clearly labeled and used only for public official statements (with proper retention). Personal accounts should be locked down (friends-only, no public location data, minimal family identifiers).

3.2 Communication Channels by Relationship

Family and Pure Friends

- Prefer end-to-end encrypted apps such as Signal (with configurable disappearing messages and minimal metadata when properly configured). Personal email is acceptable.
- Avoid ordinary SMS/iMessage for anything that could later be mischaracterized.
- **Standing rule:** “We do not discuss agency business, Council/Commission items, staff matters, or local development issues on these channels. Redirect anything official.”

Team-Related Members (Campaign Volunteers, Political Advisors, Non-Staff Supporters)

- Use dedicated campaign or pure-personal group channels (Signal or similar).
- Clear written or verbal rule that these channels are limited to strategy, outreach, fundraising, and pure political discussion.
- Official agency business is forbidden and must be redirected. Pure campaign communications that stay political are generally outside Chapter 119; mixing them creates risk.

Official Business / Constituents / Staff / Other Board Members on Official Matters

- Use only official email, official phone systems, or agency-approved tools.
- If an official matter arrives on a personal channel, forward it immediately to the official account, respond only from the official account, and treat the original as a record that may need to be retained or produced.

3.3 Daily and Weekly Behavioral Habits

- **Default filter:** “Could this reasonably relate to official agency business or a matter that may come before the body?” If yes → official channel only.
- Perform a quick morning and end-of-day scan of personal channels for accidental bleed; forward and close.
- During or near formal meetings, place the personal device on Do Not Disturb or limit non-urgent notifications.
- Never allow mixed conversations. If a personal chat drifts toward official topics, stop and redirect.
- **Deletion hygiene:** Pure personal messages may be deleted freely. Never auto-delete or routinely purge channels that might contain official content. Follow the agency’s retention schedules for anything official.
- Avoid shared family devices or cloud accounts that sync messages, photos, or location history across contexts.

3.4 Family Targeting and Doxxing Mitigation

- File public-records exemption requests under current statutory language for yourself, spouse, and children as soon as practicable. This reduces the volume of easily obtainable home-address and phone information held by government agencies.
- **Family digital hygiene education** (one short conversation plus written reminders):
 - Strict privacy settings; limit audience; disable location services and geotags on photos.
 - No posting of school names, exact schedules, real-time locations, vehicle identifiers, or “Mom/Dad is at the meeting” style content.
 - Prefer private sharing methods for family photos and updates.
 - Awareness of social-engineering and phishing (common vectors for doxxing).
- Periodic search of family names on people-search sites; request removals where possible.
- Document any threats or harassment. Florida law addresses stalking, cyberstalking, and related conduct; civil injunctions are available. In higher-threat periods, professional security consultation (physical and electronic) may be considered.

3.5 Practical Technical Hardening

- Unique strong passwords plus hardware security keys (where supported) for all accounts.
- Full-device encryption (standard on modern smartphones) plus a strong device passcode or biometrics.
- Keep operating systems and apps updated. Limit installed apps on the official side.
- Optional privacy-oriented VPN on the personal device for general browsing. Avoid any appearance that official work is being obscured.
- Backup discipline: Personal data stays in personal encrypted backups. Official data follows agency policy.

4. Suggested Implementation Sequence

1. Meet with the municipal or county attorney (and clerk) to confirm existing device policies, retention schedules, and procedures for handling official communications that may appear on private devices.
2. File exemption requests for address, telephone, and related identifying information under the current statutory framework.
3. Establish the device and account split; migrate contacts and calendars.
4. Brief immediate family and close non-official team members on the bright-line rules.
5. Create a simple one-page personal protocol for your own reference.
6. Conduct a periodic (e.g., quarterly) self-audit for accidental bleed or new apps/accounts.

5. Residual Risks and Edge Cases

- Even with careful segregation, a public records request may require the clerk or attorney to review personal channels to confirm classification. Courts examine substance, not labels.
- Campaign activity while serving in office requires ongoing vigilance to avoid mixing official and political content.
- Heated local issues increase both the volume of records requests and the incentive for opponents to probe personal channels.
- Encryption and disappearing-message features help against interception and casual over-retention, but they do not override the content-based public-records test.
- Sunshine Law violations remain possible if multiple members of the collegial body discuss foreseeable matters electronically outside a noticed meeting.

6. Closing Guidance

Strict content-based segregation enforced by technical device and account isolation, clear channel rules, family operational security, and prompt use of available statutory privacy exemptions offers the cleanest practical protection for pure personal communications while keeping the official side fully compliant. This approach is proactive rather than reactive and scales with the intensity of the political environment.

Again: This primer is general information drawn from publicly available Florida Attorney General guidance, the Government-in-the-Sunshine Manual, controlling case law, and recent statutory changes. Local implementation details (devices provided by the agency, exact retrieval procedures, precise exemption filing processes) matter. Newly elected officials should run these practices past counsel before adoption.

— End of Primer —

Prepared as a civic resource by TalkAboutMartin.com for newly elected local officials in Florida.