



## Florida Department of State

# Public Records

Brad McVay, General Counsel  
Florida Supervisor of Elections'  
Winter Conference  
December 2019

Part I

# PUBLIC RECORDS REFRESHER

# Citizens' Rights

## Florida Constitution

ARTICLE I, SECTION 24. Access to public records and meetings.—

- (a) Every person has the **right to inspect or copy any public record** made or received in connection with the official business of any public body, officer, or employee of the state, or persons acting on their behalf, except with respect to records exempted pursuant to this section or specifically made confidential by this Constitution. This section specifically includes the legislative, executive, and judicial branches of government and each agency or department created thereunder; counties, municipalities, and districts; and each constitutional officer, board, and commission, or entity created pursuant to law or this Constitution.



# Agencies' Duties

- Section 119.01(1), Florida Statutes

It is the policy of this state that all state, county, and municipal **records are open for personal inspection and copying by any person**. Providing access to public records is a duty of each agency.

- Section 119.07, Florida Statutes

Every person who has custody of a public record **shall permit the record to be inspected and copied by any person desiring to do so**, at any reasonable time, under reasonable conditions, and under supervision by the custodian of the public records.



# What Are Public Records?

Anything that is

- “[M]ade or received **pursuant to law** or ordinance or in connection with transaction of official business of agency,” Section 119.011, Fla. Stat., and
- Intended “to **perpetuate, communicate, or formalize** knowledge.” *Shevin v. Byron, Harless, Schaffer, Reid & Assocs., Inc.*, 379 So. 2d 633 (Fla. 1980).



# Any medium and anywhere

“Public records” means “**all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material.**” Section 119.011, Fla. Stat.

**Including** text messages, facebook posts, scrap paper, etc.

**On any device**: work or personal computer; work or personal cell phone, etc.

**In any location**: In your work office; in the filing cabinet in your home garage, etc.



# Public Records

## **The *Content* of The Record Determines Whether it is a Public Record**

- A record is not necessarily public if it's on a work device. For example, personal emails (unrelated to agency business) do not become public records because they were sent from a state email account.
- But a record is not necessarily personal simply because it's on a personal device.



# Public Records

## Two distinct questions

- 1) Is it a public record?
- 2) How long do we have to keep it?





# 1<sup>st</sup> Q: Is It A Public Record?

- Was it made or received **pursuant to law** or ordinance or **in connection with the transaction of official agency business, and**
- Intended to **perpetuate, communicate, or formalize** knowledge?



# Example

Type of Record: Circulated Draft of a Policy Development Memo

**Question:** Is it a public record?



# Example

**Type of Record:** Circulated Draft of a Policy Development Memo

**Answer:** Yes it is a public record because it was:

- Made in connection with the transaction of official agency business (the formulation of agency policy), and
- intended to communicate knowledge about the proposed policy (to the people to whom it was circulated).

[A]ny agency record, if circulated for review, comment, or information, is a public record regardless of whether it is an official expression of policy or marked ‘preliminary’ or ‘working draft’ or similar label.”

*Government-in-the-Sunshine Manual*, 2019 Ed.,

[http://www.myfloridalegal.com/webfiles.nsf/WF/MNOS-B9QQ79\\$file/SunshineManual.pdf](http://www.myfloridalegal.com/webfiles.nsf/WF/MNOS-B9QQ79$file/SunshineManual.pdf)



# Example

**Type of Record:** Personal Notes Regarding a Policy Meeting

**Question:** Is it a public record?



# Example

## Type of Record: Personal Notes Regarding a Policy Meeting

**Answer:** No, it is not a public record because:

- The notes were made in connection with the transaction of official agency business (attending a policy meeting), **but**
- They were not meant to perpetuate, communicate, or formalize knowledge (because they were only intended for the personal use of the drafter).
- “[U]nder chapter 119 public employees’ notes to themselves which are designed for their own personal use in remembering certain things do not fall within the definition of ‘public record.’” *The Justice Coal. V. the First Dist. Court of Appeal Judicial Nominating Comm.*, 823 So. 2d 185 (Fla. 1st DCA 2002) (noting public records include only those that “perpetuate, communicate, or formalize knowledge”).



## 2<sup>nd</sup> Q: How Long Do We Have to Keep Them?

- **Agencies *may not destroy or discard* public records *except* pursuant to the applicable *Retention Schedules*.**
- “Each agency shall comply with the **rules establishing retention schedules and disposal processes for public records** which are adopted by the [Division of Library and Information Services of the Department of State].” § 119.021, Fla. Stat.
- “Public records may be destroyed or otherwise disposed of **only in accordance with retention schedules** established by the Division.” Rule 1B-24.003.
- **NOTE:** Consult with your county attorney to confirm there are no **litigation holds** before destroying records.



# Cont'd

- **Every Public Record by necessity must fall under a retention schedule; otherwise, the agency would be required to keep it.**
- ***You may not destroy the record just because you can't determine which schedule it falls under.***
- “the Division [of Library Services] shall establish a time period for the retention or disposal of each series of records.” § 119.021, Fla. Stat.
- Agencies must **document** the destruction of records that have met retention.



# Records Retention Schedules

- “The [Department of State] issues **General Records Schedules** which establish *minimum* retention requirements for record series common to all agencies or specified types of agencies based on the legal, fiscal, administrative, and historical value of those record series to the agencies and to the State of Florida.” **Rule 1B-24.003.**
- The General Records Schedule GSI-SL for State and Local Governments can be found here:  
<https://www.flrules.org/Gateway/reference.asp?No=Ref-04998>





# Example

**Type of Record:** Policy Development Memo

**Question:** How long are we required to keep it?



# Example

**Type of Record:** Policy Development Memo

**Answer:** Retain for 5 fiscal years.

“CORRESPONDENCE AND MEMORANDA: PROGRAM AND POLICY DEVELOPMENT Item #338

This record series consists of correspondence and memoranda documenting policy development, decision-making, or substantive programmatic issues, procedures, or activities...These records may have archival value.

**RETENTION:** 5 fiscal years. ***State agencies must contact the State Archives of Florida for archival review before disposition of records...***



# Public Records

- A person who requests a public record is not required to show a legitimate or non-commercial interest as a condition of access to the record.
- An agency may not require that the public records request be in writing or even require the requestor to identify himself or herself, unless specifically authorized by statute.
- The Public Records Act does not contain a specific time limit to provide requested records but Florida courts have determined records must be produced in a reasonable time that would allow the custodian to retrieve the records and redact any exempt information.



# Unreasonable Delay

- “A custodian of public records and his or her designee must **acknowledge** requests to inspect or copy records **promptly** and **respond** to such requests **in good faith**. § 119.07, Fla. Stat.
- The law allows agencies a reasonable time during which to make “reasonable efforts to determine from other officers or employees within the agency whether such a record exists and, if so, the location at which the record can be accessed,” and to determine whether “all or part of the record is exempt from inspection and copying.” *Id.*



# Unreasonable Delay

- **Florida law does not set forth a *specific number of days* during which to fulfill a request.**
- **You are not required to provide the requestor with a specific date the production will be complete.**
- Make every effort to acknowledge the request as promptly as possible, preferable within one day to the extent possible under the circumstances.
- Fill it as quickly as reasonably possible.



# No Requirement Under Chapter 119 to:

- Reformat records to suit the requestor's needs.
- Create records that do not exist.
- Respond to information requests (e.g., answer questions about information in records).
- Perform research for a requestor.
- Respond to a “standing” request.



# Agencies May Charge . . .

- For extensive use of agency resources.
- Copying costs, plus staff time.
- Begin work after receipt of payment, unless special circumstances dictate otherwise.
- The calculation of costs is set forth in **statute, rule, and policy**. See section 119.07(4)(d), Fla. Stat., as a starting point.
- Please consult your county attorney for details regarding the calculation of costs.



# Public Records Best Practices

- “Tag” confidential or exempt emails when you write them.
- For large requests, records can be released in batches as they become available (a rolling production) if the circumstances warrant it.
- Keep a single point of contact with the requestor.





# Traps for the Unwary

- **Some requests may seem like irrelevant spam.**
- ***Don't ignore them.*** The following is an actual request that led to a lawsuit:

PUBLIC RECORDS REQUEST TO [NAME OF EMPLOYEE]: This public records request comes from a citizen of the State of Florida. Please promptly forward every work email that you SENT (this does not include the emails you RECEIVED) on, 4/8/13, during the time period starting at 8:00 a.m. and ending at 12 noon. Please simply forward any such emails to me electronically at the email address that this public records request was sent from ([ERIK@4CONSUMERRIGHTS.COM](mailto:ERIK@4CONSUMERRIGHTS.COM)). If you contend that you are not going to send me any of these emails for any reason, please send me those reasons (by email) in writing with particularity. Thank you.



# Public Records Violations

One of the results of failing to comply with a Public Records request is a civil action being filed against an agency for refusal to allow a public record to be inspected or copied, which could result in reasonable costs of enforcement, including attorneys' fees, being assessed against the agency.



# Public Records Violations

Violations may also be assessed against an individual.

Section [119.10\(1\)](#) Violation of chapter; penalties.

(1) Any public officer who:

(a) Violates any provision of this chapter commits a noncriminal infraction, punishable by fine not exceeding \$500.

(b) Knowingly violates the provisions of s. [119.07\(1\)](#) is subject to suspension and removal or impeachment and, in addition, commits a misdemeanor of the first degree, punishable as provided in s. [775.082](#) or s. [775.083](#).

(2) Any person who willfully and knowingly violates:

(a) Any of the provisions of this chapter commits a misdemeanor of the first degree, punishable as provided in s. [775.082](#) or s. [775.083](#).

(b) Section [119.105](#) commits a felony of the third degree, punishable as provided in s. [775.082](#), s. [775.083](#), or s. [775.084](#).

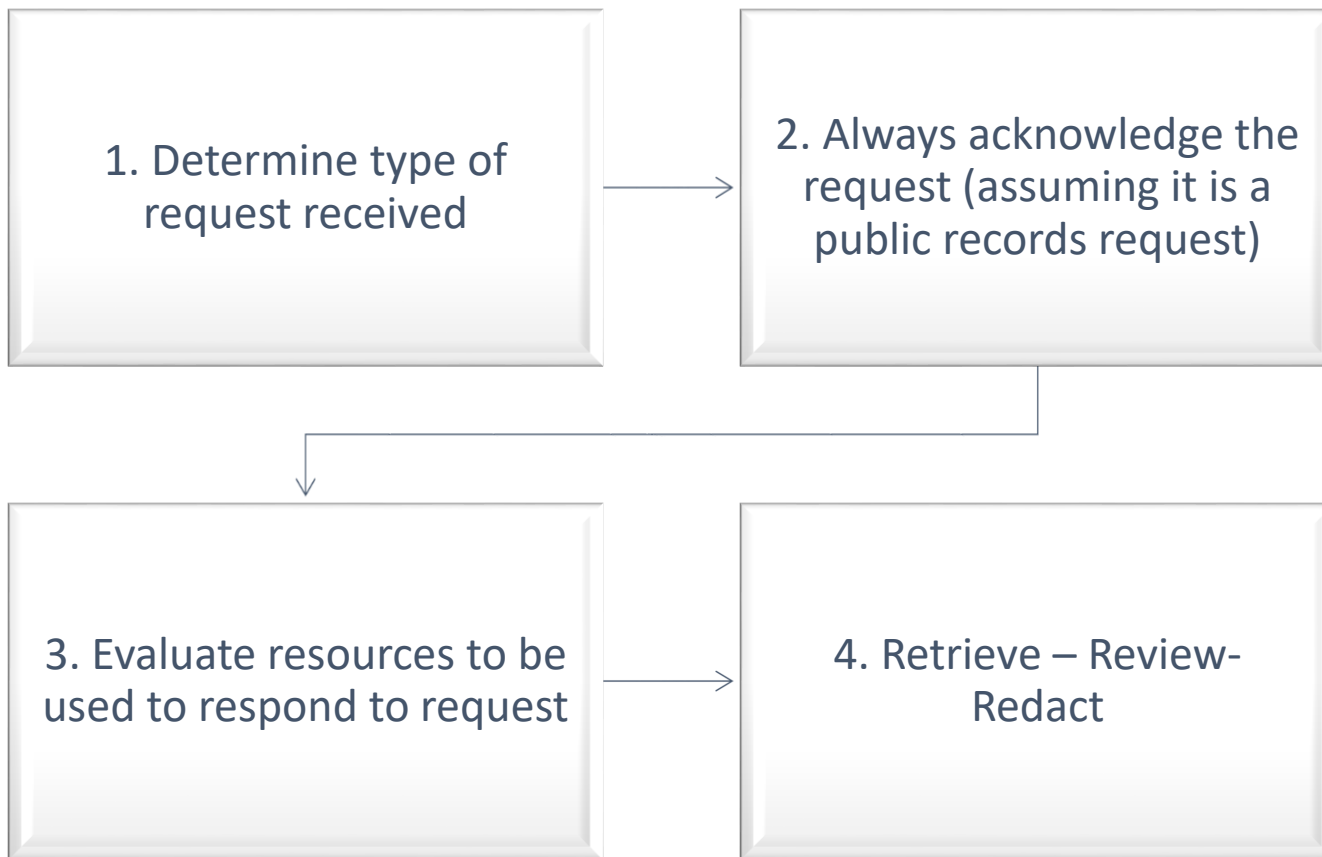


Part II

# PROCESS FOR RESPONDING TO PUBLIC RECORDS

# The Process

This is process we use at DOS. There are certainly other ways to process public records requests, so by no means am I suggesting this is the only way to process requests. Use what works best for your organization.



# Step 1

Determine what type of request you received.

- Question: Is it actually a public records request that triggers a legal obligation to respond under section 119, Fla. Stat., or a request for information?
  - If yes, a public records request, proceed to step 2.
  - If no, you have no legal obligation to respond to requests for information. You may wish to do so for other reasons, but ch. 119 wouldn't apply.



# Step 2

## Acknowledge the Request

- Do so promptly – see slide 30.
- Although no specific time requirement in the statute, it is good practice to try to acknowledge a request as soon as possible, preferably within 24-48 hours.



# Step 3

Evaluate the time and resources to be utilized to respond to request (invoice if necessary)

- Questions you or your PRR custodian should be asking at this stage:
  - ✓ Who in organization would have responsive records
  - ✓ How will you go about obtaining those records (email/desktop search, data pull, audio file, etc.)
  - ✓ How many resources will need to be used to fulfil this request (staff time, review of documents, etc.)
  - ✓ If extensive use of resources – over 30 minutes to fulfil, you can invoice (begin work after receiving payment before proceeding to Step IV)

If no invoice is going to be sent, proceed to Step IV





# Step 4

## Retrieve, review and redact

- Locate all responsive records
- Review those records
- Redact as appropriate



# Analyze the request

**Example 1:** Did you communicate with other Supervisors of Elections or the Division of Elections prior to seeking legislative funding for conducting straw polls in municipal elections? Please provide any and all relevant documents, records, communications, etc.

**Question:** Is this a public records request?



# Analyze the request

**Example 1:** Did you communicate with other Supervisors of Elections or the Division of Elections prior to seeking legislative funding for conducting straw polls in municipal elections? Please provide any and all relevant documents, records, communications, etc.

**Question:** Is this a public records request?

**Answer:**

- Part of this is a request for information and part of it is a records request. You may, but are not required to, respond to a request for information.
- If there are responsive records, you would proceed accordingly under the public records analysis. If there are not responsive documents, you would simply state “no responsive records” or something similar.



# Analyze the request

**Example 2:** How did you utilize Facebook, Twitter, Instagram, Snapchat, LinkedIn, and Nextdoor to publicize the extended voting hours as directed by court order?

**Question:** Is this a public records request or a request for information?



# Analyze the request

**Example 2:** How did you utilize Facebook, Twitter, Instagram, Snapchat, LinkedIn, and Nextdoor to publicize the extended voting hours as directed by court order?

**Question:** Is this a public records request or a request for information?

**Answer:**

- No. This is a request for information.
- While you are certainly free to respond with information and/or provide copies of any applicable social media postings on the topic should you wish to do so, the public records law would not apply.



Part III

# SPECIFIC EXEMPTIONS

# Exemptions – What can be withheld?

- Must be a specific listed exemption in Florida Statutes, or must be designated in federal law (*i.e.*, HIPAA records).
- Must redact the protected information from the record and release the rest, unless the nature of the record is such that the whole thing must be withheld.



# “Exempt” v. “Confidential”

- An agency is not required to release **exempt** information to the public, but is not prohibited from doing so.
- An agency is prohibited from releasing **confidential information** – often by threat of civil or criminal liability – unless by court order, consent, or statutorily-specified process.
- The language of an exemption will generally state whether the information is exempt and confidential or, alternatively, will only refer to the information as being exempt.





# Common Exemptions

## **Exempt:**

- Certain personal information (*e.g.*, home addresses) of specified high-risk employees (who have specifically requested that their information be withheld); certain blueprints.

## **Confidential and exempt:**

- SSNs; certain medical information; certain financial records; trade secrets; security system plans.



# Notice That Information Is Being Withheld

- Agencies are required to notify the requestor and describe the nature of information that is being withheld due to its exempt or confidential status.
- The notice to the requestor must include the specific statutory exemption for each portion of information withheld.



# Cybersecurity Information Sharing Act of 2015

## (CISA) (6 U.S.C. § 1501-1510)

- The Act provides a basis in federal law for state and local governments, as well as private entities, to share, for a “cybersecurity purpose,” specific information used to protect information systems and information, and exempts such information from Sunshine Law disclosure. § 1503(d).
- “**Cybersecurity purpose**” is defined as “the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.” § 1501(4).
- The exemption applies to “**cyber threat indicators**” or “**defensive measures.**” § 1501(6),(7).



# Cyber threat indicator

- The term “**cyber threat indicator**” means information that is necessary to describe or identify—
    - (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering information related to a cybersecurity threat or security vulnerability;
    - (B) **a method of defeating a security control or exploitation of a security vulnerability;**
    - (C) a **security vulnerability**, including anomalous activity that appears to indicate the existence of a security vulnerability;
    - (D) **a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;**
    - (E) malicious cyber command and control;
    - (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
    - (G) **any other attribute of a cybersecurity threat**, if disclosure of such attribute is not otherwise prohibited by law; or
    - (H) any combination thereof.
- § 1501(6) (emphasis added).



# Other Key Terms

## Security Vulnerability

- A “security vulnerability” means “any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.” § 1501(17).

## Defensive measure

- A “**defensive measure**” is defined to include “an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.” § 1501(7).



# Key Points

- Information is not directly related to a cybersecurity threat (and thus not exempt) if it is not necessary to prevent, or mitigate the cybersecurity threat. For example, the substance of and sender information related to a spear phishing email could be considered directly related to a cybersecurity threat; while the name and e-mail address of the target(s) of the email would be personal information not directly related to a cybersecurity threat and not typically included as part of the cyber threat indicator. See [https://www.us-cert.gov/sites/default/files/ais\\_files/Non-Federal\\_Entity\\_Sharing\\_Guidance\\_\(Sec%20105\(a\)\).pdf](https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_(Sec%20105(a)).pdf).
- A defensive measure could be something as simple as a security device that protects or limits access to an organization's computer infrastructure or as complex as using sophisticated software tools for vulnerability scanning. See *id.* Similar to a threat indicator, a defensive measure will generally consist primarily of the technical information that can be used to detect and counter a cybersecurity threat. See *id.*

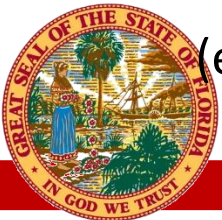


# Physical security exemptions

- § 281.301, Florida Statutes provides:

**(1) Information relating to the security or firesafety systems** for any property owned by or leased to the state or any of its political subdivisions, and information relating to the security or firesafety systems for any privately owned or leased property which is in the possession of any agency as defined in s. 119.011(2), including all **records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to or revealing such systems or information** is **confidential** and **exempt** from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, and any portion of a meeting relating directly to or that would reveal such systems or information is exempt from s. 286.011 and s. 24(b), Art. I of the State Constitution, and other laws and rules requiring public access or disclosure.

(emphasis added).



# Physical security exemptions (cont.)

- The § 282.301 exemption was clarified and recreated in § 119.071, Florida Statutes, during the 2001 Legislative session. § 119.071(3) provides for the exemption and confidentiality of, among other things:
  - A security system plan or portion thereof; and
  - Building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout and structural elements of a building.
- The term “security system plan” includes all “[r]ecords, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to the physical security or firesafety of the facility or revealing security or firesafety systems.” § 119.071(3)(a), Fla. Stat.





# Application of physical security exemption

- The Fifth District Court of Appeal, in *Central Florida Regional Transportation Authority d/b/a Lynx v. Post-Newsweek Stations, Orlando, Inc.*, 157 So. 3d 401 (Fla. 5th DCA 2015), considered whether security tapes from cameras installed on transportation authority buses were confidential as revealing the security system.
- The court held that the footage was confidential under section 281.301, Florida Statutes, because it directly related to and revealed information about a security system. *Id.* at 405.
- Significantly, the court noted that the videos “which are records, reveal the **capabilities**—and as a corollary, **the vulnerabilities**—of the current system.” *Id.* at 405. (emphasis added).



# Resources

Florida Office of the Attorney General

Open Government Website

<http://www.myfloridalegal.com/pages.nsf/Main/314BA231F89C0C8A8525791B006A54E2>

- The website includes many resources, including the Government-In-The-Sunshine Manual which incorporates laws, judicial decisions, and Attorney General opinions in place as of the year prior to publication.





# FLORIDA DEPARTMENT *of* STATE

For more information, visit us online at:  
[dos.myflorida.com/elections/](https://dos.myflorida.com/elections/)

