

The following information was provided on November 27, 2017, by the Bureau of Library Development, Division of Library and Information Services.

Snapchat and Records Retention

The Nature of Snapchat

Snapchat is designed to share brief communications, or “snaps,” consisting of photos, videos or messages that, once viewed, quickly self-destruct. As soon as a user sends a snap, the user no longer has access to it and cannot retrieve it in any way. Once a contact views a snap, it disappears after no more than 10 seconds and cannot be retrieved by anyone. Snaps that a contact does not open disappear from the Snapchat server after 30 days.

A user can post a snap to their “story,” which saves the snap for 24 hours before it self-destructs.

A user can also save a snap to their “memories,” which prevents it from automatically being deleted. These snaps are retained on Snapchat’s server for an undetermined period of time.

Public Library Records Retention Requirements

All public libraries in Florida are public agencies as defined in *Florida Statutes*. As public agencies, public libraries are required by Florida’s Public Records Law to manage records of their operations and to retain those public records in accordance with records retention schedules established by the Department of State. Records retention schedules indicate the minimum period of time that public agencies are required to retain various categories of public records.

For public libraries, records retention requirements can be found in [General Records Schedule GS1-SL for State and Local Government Agencies](#) and [General Records Schedule GS15 for Public Libraries](#). The GS1-SL sets forth retention requirements for administrative records common to all agencies, such as personnel records and correspondence files. The GS15 provides retention requirements for records specific to libraries, such as circulation records.

Retention of Social Media Posts

Records retention periods are determined by the content, nature and purpose of the records and are set based on the records’ legal, fiscal, administrative and historical values, regardless of the method by which they are created or transmitted. For that reason, there is no single retention period that might apply to all social media posts, including snaps. We advise all public agencies, including public libraries, to carefully consider public records access and retention requirements, responsibilities, and implications when thinking about using any social networking technologies.

Within our own department, social media is typically used for general communication to the public about our programs, services and events. Such records fall under the item called “Public Information Files” in *General Records Schedule GS1-SL*, which has a minimum retention of 90 days. However, even a 90-day retention requirement is far longer than snaps can be retained

unless they are saved to “memories,” and even this option does not ensure the required retention or accessibility of the records. Therefore, public agencies need to exercise great caution when considering whether or how to utilize Snapchat. If there is no way for a public agency to retain or access the records of its communications, the agency is not in compliance for those public records.

Contact Us

If you have any questions about managing your records, please contact the Division of Library and Information Services' Bureau of Archives and Records Management at recmgt@dos.myflorida.com.

Snapchat Resources

The articles below discuss Snapchat, especially as it's used in business settings.

[DiDomenico, Pat. "Snapchat for Business: Beware the Legal Risks of Self-Destructing Texts." *Business Management Daily*. 14 Feb. 2014.](#)

Gives business professionals a legal view on messages that are sent over media types designed to leave no evidence.

[Isajiw, Peter J., and John C. Vázquez. "United States: Issues With Self-Destructing Messages in the Workplace." *Mondaq*. 12 Mar. 2014.](#)

Discusses compliance and other concerns.

["Social Media and the Law: A Handbook for UK Companies." *Linklaters*. Jan. 2014.](#)

Provides a general understanding of best practices (not UK-specific).

["This Article Will Self-Destruct: Your Employee's Use of These ESI-Destroying Apps Could Subject You to Sanctions." *Polsinelli*. June 2014.](#)

Discusses the need to be able to preserve material for defense against accusations.