

Playbook for Governors on State and Territorial Government Records

The Council of State Archivists (CoSA) is the membership organization of the 56 state and territorial archives, and offers detailed information and resources pertaining to government records management and archives. CoSA can help the Governor's office connect with their appropriate state agencies. A state-by-state directory of archival and records management agencies can be found at: <https://www.statearchivists.org/connect/resources-state/>

Play #1 Government Service is Different

Elected officials and their staff entering public service for the first time need to understand that government work is documented and preserved differently from that in the private sector, because of the government's obligations to its citizens. Government records are those created or received by the Governor, immediate staff, and other units and individuals in the Governor's office, in the conduct of government business. Generally, government records are considered the property of the state or territory even if they are created and kept on your personal devices, if the records pertain to the public's work. Your work as a public servant creates public records that must be managed, transferred, and preserved.

Play #2 Government Records Are Subject to Law

State and territorial law, statute, and regulation require that Governors and their staff properly manage state government records. These obligations begin on Day One of an administration, and ideally at the point of election. Contact the state or territorial archives staff for an educational overview about records management expectations and obligations in your state or territory. Your state or territorial archivist and archives staff will be able to update your staff and cabinet or department officials about the laws, statutes, and regulations that govern the records created as part of public service.

Public information is subject to public records law -- no matter where it is created or held. That means private email accounts are subject to public records requests and freedom of information requests if they are used to conduct public service.

Play #3 Managed Records Are Assets. Unmanaged Records Are Risks.

State and territorial archives and records management are central to the usefulness of state government actions, programs, and policies. In order to manage the public records your administration creates, establish communication and relationships with your state or territorial

archives. They will help you ensure that your records are properly handled, including management, maintenance, long-term retention or archival transfer, and appropriate destruction.

It is critical to preserve government records for the appropriate amount of time as specified under state law or statute and in records retention schedules and policies. State archives and records management personnel can help you and your staff determine what qualifies as a record. While laws vary from state-to-state, a record normally is a piece of information that documents an organization's "functions, policies, decisions, procedures, operations" or other significant activities. Some records do not need to be maintained long-term, so disposing of records when appropriate minimizes the amount of data that needs to be stored. When the records management schedule indicates that it is appropriate to dispose of or delete records, do so immediately.

- **Identify records**
- **Transfer records to the archives, as required**
- **Delete non-records**

Play #4 Start Managing Records Right Away

Communications generated during transitions into and out of office and communications using private email, cell phones or any electronic communication relating to public business often qualify as public records. These records need to be managed even before public service officially starts.

Organization now prevents loss of information later. Talk to your state or territorial archives about naming conventions for files, software choices, and other concerns you may have about creating, organizing, and transferring state government records during your service.

Establish records management procedures and practices that are guided by state law and regulation from Day One. This will help your office:

- Provide documentation for gubernatorial papers and their eventual transfer
- Know where to find records
- Destroy records when legally authorized
- Respond to information requests
- Manage records for historical purposes

Seek guidance from your state archives or records management agency regarding appropriate records retention policies and disposition schedules to be used for your records. These guidelines are typically already developed and in use. Your state archives or records management agency will help you make sure your office policies are in keeping with state or territorial requirements.

Have your team agree on policies, procedures, and rules for creating and sharing information in your office and the offices of your cabinet. Make sure everyone knows about:

- ***Naming conventions***
- ***File organization***
- ***Version control.***

Play #5 Public Records Requests

Government service creates public records. The public has the right to request access to records through public records or freedom of information requests. Be prepared for frequent public records requests for access to copies of records including, electronic records. Be prepared for frequent requests for email and text messages. Organizing government records and managing them properly will make it easier and less time-consuming to fulfill these requests. Be prepared to invest the staff resources needed to review large volumes of email to determine whether it is protected from or subject to public disclosure. State governments have a variety of freedom of information legislation and statutes. The requirements to release information, how exempt information is identified and classified, and how requests are processed varies from state to state -- therefore, you should contact your state or territorial archives and work with your legal counsel to become familiar with the laws in your jurisdiction pertaining to public access or restriction requirements in your state or territory.

Play #6 Protect Your Privacy -- Keep Private Messages on Private Accounts and Public Messages on Public Accounts

Most states and territories have laws and statutes that treat public information on any account as a public record. This means that if you use your private accounts to send messages pertaining to your work in government that your private accounts will be subject to public records or freedom of information requests. Likewise if you use the accounts you have been assigned as a public servant to carry out your government duties to discuss private information, that information might be released during an authorized public records review. Protect your privacy and make managing the public records easier for yourself and your office. Use your private accounts for private information and your public accounts to communicate about public responsibilities.

Play #7 Social Media in Government

Social media platforms are a powerful way to communicate government information directly to the public. Like so much of government service, use of social media in government needs to be handled differently than in the private sector.

A social media policy will need to be regularly reviewed and refined by a social media team. This group, likely in the Governor's communications office, should include social media staff, managers, and content creators. The social media team should consult with the Governor's legal counsel and the state/territorial archives and records management staff to make sure that policies and practices are consistent with state/territorial law and statute.

Your office will need to:

- Understand that social media is a public record. This means you will need to regularly transfer social media records to the appropriate agencies according to the records retention policies of your state or territory.
- Comments or messages made by the public on social media platforms may also be subject to public record laws.
- Develop or update a social media policy for your office and employees that adheres to state/territorial law and statute. Your legal counsel and state/territorial archives can help.
- Review terms of service agreements for social media to make sure that government requirements are met. Work with your IT to determine if there is an enterprise-level agreement with the social media vendor that meets the standards of the state and covers all appropriate provisions.
- Maintain official accounts for official information
- Only use official government social media accounts for official business (keep personal information on personal accounts).
- Use campaign accounts for campaigning and official accounts for official business.
- Hand off government social media accounts from one administration to the next to maintain consistency and integrity.

Play #8 Email and Text Messaging

Email is one of the most important electronic communication tools in the workplace, including in state government business. Identifying emails that are permanent or long-term electronic records within an email account and properly managing them for long-term use is an important responsibility.

Any communication account used for state business is subject to public records laws. If personal accounts are used for government business, the content about public service is a public record. To simplify, be sure that all public officials use official media accounts for state business. It is best practice to avoid using personal email, social media, or other messaging accounts when creating public records. If government business must be conducted on personal accounts, the public records created should be transferred as soon as possible from personal accounts and devices onto secure government-owned servers or hosted cloud services.

Contact your state or territorial archives for more information on transfer and records management practices. The state archives or records management agency can also help assess and evaluate collaborative environments (for example Jira, Slack, Trello, and other remote communication platforms), and help your organization make decisions about how to use these platforms in effective ways while also protecting and managing records.

Play #9 Public Records and Remote Work

As a cost-saving measure, in response to the pandemic, and even to attract skilled workers, government has been increasingly shifting to remote work. This can be a major benefit for continuity in government, but it also raises challenges around good records management practices. Public records are records created and received by government officials in the course of performing government business whether that is on personal computers, cell phones, or online using SaaS (Software as a Service) document-sharing platforms.

A records management best practice is to keep public information off private accounts and devices. Sometimes in remote work situations that is not possible. In cases when records must be stored on a personal device, they should be kept in separate, labeled folders. They should be backed up and transferred to the appropriate agency or archives storage location as soon as possible. Records held at home are subject to the same processes and protections as when they are in the office.

Cybersecurity Tips:

- All devices, networks, and accounts used to access public records should be protected with strong passwords of at least 8 characters.
- Home routers should be password protected and have up-to-date security patches.
- Records with personally identifiable information (PII) such as Social Security Number, date of birth, etc. and other confidential information should only be handled in a home office with special permission.
- If your agency or organization offers a virtual private network (VPN), protected government records should be accessed via the VPN as it is the most secure option.
- Avoid publicly available Wi-Fi networks. They are not secure, even if accessed through a government issued device.
- Contact your departmental or state IT department for the most up-to date information on cybersecurity.

Play #10 Transitioning Out -- the Final Play

When your time in public service ends, you will still have responsibility for properly managing the government records created while you were in office. You will need to:

- Plan for continuity of operations.
 - Identify and maintain public records necessary for the incoming official. Consult with your state archives and records management agency to understand public records management obligations and policies. Plan for the transfer of public records.
- Follow established records retention schedules and policies.
 - Transfer permanent public records to the appropriate repository as designated by law or past state practices.
- Officials should return all state-owned devices such as cell phones, laptops, storage devices, etc. as required by established state policies and procedures, and ensure that public records stored on those devices are transferred properly.
- Electronic communication accounts including, but not limited to, Twitter, Facebook, Instagram, or others should be handed over to the incoming officials.

CoSA
PO Box 1583
Frankfort, KY 40602-1583
502.229.8222
www.statearchivists.org

NGA
444 N. Capitol, NW, Suite 267
Washington, DC 20001
(202) 624-5300
www.nga.org

Support for CoSA's contributions to this publication was provided by the National Endowment for the Humanities Coronavirus Aid, Relief, and Economic Security (CARES) Act.