Public Records and Remote Work:

Advice for Government Agencies

Agencies and organizations have adopted remote work at an exponential rate as technology has made more kinds of work possible from outside the office and as the pandemic has required a shift in practices to encourage distance. State, regional and local government employees are teleworking at unprecedented rates -- the majority of states and territories have at least some employees working remotely. This is a major benefit to continuity in government during the pandemic, but it also raises some challenges around good records management practices.

Employees should always follow their agency's policies and procedures on telework. This document highlights best practices for complying with records management laws and statutes. Contact your state or territorial archivists or records managers if you have questions about your state's requirements and how to follow them.

No Matter Where They Are Created Public Records are Public Records

Public records are records created and received by government officials in the course of performing government business. Government employees, whether appointed, hired, or elected, create public records that document government actions, policies, and activities. Each state has laws, statutes, or regulations that define public records as they are created and then kept or preserved for a period of time. Public records can be created at the city, county, state, or federal government level and may include documents, maps, recordings, films, photographs, court cases, or other materials regardless of format. Increasingly, public records are created and maintained in electronic formats.

Public records created on personal computers, cell phones, or online using SaaS (Software as a Service) document-sharing platforms are all still public records.

Public records created in the course of public business are subject to records management and open records laws and statutes no matter where they are created or stored. Public records created and maintained in a home office, the cloud, or even on social media platforms must follow proper retention and disposition schedules. For example: if an employee saves minutes of a virtual meeting on a personal or home computer, or on a document sharing platform on the cloud, those minutes are still subject to public records laws and statutes.

Where to Store Electronic and Paper Records When Working at Home

Best practice is to separate public records and personal records when working. Whenever possible, employees should store electronic public records on government-issued devices, drives, or cloud-space (i.e. SharePoint, OneDrive, shared SaaS drives such as Google Drive or Dropbox).

Public records in paper format should be kept separate from personal records in a home office. As much as possible, it is recommended to conduct business electronically. Paper files that must be used for teleworking should be returned to the proper work office environment as soon as practical. If physical records are scheduled to be destroyed before an employee can return to their office, the employee should check with their supervisor before destruction, track what is being destroyed, and make sure all records are destroyed in accordance with state regulations. The records should not be placed or mixed with home recycling. Electronic files should be permanently deleted and not simply moved to a computer's recycle bin. Work with your IT department to properly perform a complete data wipe on sensitive records.

If 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.

Email, Messaging, and Social Media

Email or social media accounts used for state business are subject to public records laws. If personal accounts are used for government business, the content created is a public record. To simplify your compliance, 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 an employee must use a personal account to work on a public record, they should understand that they are responsible for the maintenance and security of that record, and it can still be requested through a government transparency request.

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 and onto secure government-owned servers. Contact your state or territorial archives for more information on transfer and records management practices. The state archives or records management unit 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 permanent records.

Government Transparency and Public Right to Know

Public records created on personal devices are subject to state and federal government transparency laws and regulations. If there is a request for public records created on a personal device, the employee will be responsible for locating and transferring them to the appropriate party. Agencies can make non-confidential records publicly available on their website to ensure that information is widely available to the public.

Public Records Security at Home

Working from home has security concerns. It is the employee's responsibility to protect public records and sensitive information stored on telework or personal devices. It is the employee's responsibility to protect the information transmitted on external networks. Unauthorized people, including family members, should not have access to sensitive public records stored at home. Public records are made available based on retention schedule, need, and regulations governing those records. **Records held at home are subject to the same processes and protections as when they are in the office.** Employees using personal devices to access public records should make sure those devices are password protected, locked, and secure at all times. Employees should take extra care to avoid viruses and other malware threats. If a personal device is compromised, even after work hours or in the course of non-work-related activity, it can impact public records or agency networks that have connected to that device as well.

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 SSN, 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 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 and teleworking.

Avoid Phishing Attempts

Employees commonly face phishing attempts at the office as well as when teleworking. Phishing is when someone represents themselves as a trusted source to trick a user into revealing private information. Phishing usually occurs through email but can also come as phone calls, text messages, and in social media. Phishing emails may contain links or attachments that install malicious software when they are opened. Links may also take users to fake websites or forms to collect personal information, such as usernames, passwords, and account numbers. To avoid phishing attempts:

- Watch out for unauthorized attempts to gain access to accounts.
- Watch for emails asking for personal information and remember to always keep passwords private. IT personnel will never ask for any password.
- Verify links before clicking on them.
- Check for red flags such as strange email addresses, slight misspellings in hyperlinks, or emails stating you have an account or you've opened an account when you don't remember doing so.
- Check the legitimacy of urgent emails that request immediate action before responding.
- Never open attachments or links from unknown people or companies.

Additional Resources

Telework in Pennsylvania: Best Practices (Pennsylvania State Archives)

Best Practices for Cloud Computing Records Management Considerations (North Carolina Division of Archives and Records)

Protecting PII: Telework Best Practices (U.S. Department of Homeland Security)

Telework Guidance: Security and IT (U.S. Office of Personnel Management)

PA Protecting Yourself Online Guide (Pennsylvania Office of the Governor)

About CoSA

Formed in 2002, the Council of State Archivists (CoSA) is a national nonprofit using collaborative research, education, and advocacy to provide leadership that strengthens and supports state and territorial archives in their work to preserve and provide access to government records. Its members comprise the state archivists in the 50 state, 5 territorial and District of Columbia archives. These individuals oversee agencies that hold a legal mandate to document government and protect the rights and history of the American people across our country.

Support for this publication was provided by the Institute of Museum and Library Services (IMLS) through a National Leadership Grant to the Council of State Archivists (CoSA) for Archives Collaborating and Cooperating with External Strategic Stakeholders (ACCESS), a project of the State Electronic Records Initiative (SERI).

The Pennsylvania State Archives leaflet on managing public records while working remotely inspired and informed this document. CoSA acknowledges the contributions and support of the Pennsylvania State Archives in the development of this document.

September 2020

CoSA
Council of State Archivists
DOCUMENTING GOVERNMENT · PROMOTING HISTORY · SECURING RIGHTS

COUNCIL OF STATE ARCHIVISTS
PO Box 1583 • Frankfort, KY 40602-1583
502.229.8222 | www.statearchivists.org