Pennsylvania State Archives
PENNSYLVANIA HISTORICAL & MUSEUM COMMISSION

Telework in Pennsylvania: Best Practices

Technology makes working remotely possible but also presents issues for records management. As state employees transition to telework on a partial or full-time basis, they should consider good records management practices.

Employees should always follow their agency's internal policies and procedures on teleworking, and the advice in this leaflet should help workers comply with Pennsylvania records laws and records management best practices.

Records Made at Home are Still Public Records

Management Directive 210.5 *The Commonwealth of Pennsylvania State Records Management Program* states all records created in the course of official business are public records no matter where they are created or stored.

Public records created and maintained in a home office are still subject to Right to Know requests and must follow Commonwealth retention and disposition. Likewise, if a record is created on a personal computer or other device in the course of official business it is still a public record. For instance, if an employee types and saves the minutes of a virtual meeting on a personal computer at home, those minutes are still public records.

As a general rule, public records and personal records should be kept separately when working from home. Employees should store electronic public records on government-issued devices(i.e. SharePoint, OneDrive or shared drives). If records must be stored on a personal device, they should be kept in separate folders on that device, backed up, and transferred to an agency storage location as soon as possible. Paper files should be kept physically separate from any personal records in a home office.

Paper and Electronic Records

Conduct business from home electronically as much as possible. Paper files that are needed for teleworking purposes should be and returned to their proper place in the work office as soon as practicable.

Commonwealth policy allows non-permanent public records to be kept in electronic form. Instructions for keeping records with permanent retention can be found in the Policy Regarding Agency Long Term and Archival Records in Electronic Format.

Email, Messaging, and Social Media

If possible, employees should use work accounts for any email or instant messaging relating to government business. Employees should not use personal email, social media, or other messaging accounts when creating, revising, or reviewing 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 that it can still be requested through a Right to Know request. All such records should be transferred as soon as possible off of personal devices and onto secure commonwealth-owned servers.

OneDrive and Other Cloud-Based Record Systems

OneDrive is an online cloud storage space available to many commonwealth and local government employees using Office365. Records stored in this space can be accessed easily from outside the office and shared with other employees and contacts.

Keep in mind that electronic records stored in OneDrive or other cloud-based storage locations require active management by their record creators. OneDrive is not intended for permanent or long-term storage of public records.

Employees should avoid storing public records solely on their OneDrive account. A OneDrive account is tied specifically to an individual employee's authenticated account and is not accessible to other employees or IT professionals. When an employee leaves commonwealth service or transfers between agencies their OneDrive records are moved to an archive site for 30 days and then deleted automatically. Employees should make sure that public records created in their own OneDrive accounts are accessible in networked storage such as a shared drive or SharePoint site.

Right to Know

If employees create, review, or maintain public records on their personal devices, or through any personal accounts, those records are still subject to Right to Know requests. If a Right to Know request requires documents on an employee's personal device or account, that employee will be responsible to produce them.

If an employee creates and maintains public records on a personal device, non-work related and personal files on that device are not considered public records and are not subject to Right to Know requests.

When possible, agencies are encouraged to promptly make copies of non-confidential records publicly available on their websites, eliminating the need for Right to Know requests which can be difficult to complete when employees are teleworking and records are not easily accessible.

Public Records Security at Home

Publicly available Wi-Fi networks are not secure, even if accessed through a government issued device. Employees should not access any confidential documents while using public Wi-Fi.

Employees using personal devices should make sure they are password protected, locked, and secure at all times.

Employees should take extra care to avoid phishing, viruses, or 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.

Employees should:

- Watch out for unauthorized attempts to gain access to their accounts.
- Watch for emails asking for personal information and remember to always keep their 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 or slight misspellings in hyperlinks
- Check the legitimacy of urgent emails that request immediate action before responding.
- Never open attachments or links from unknown people or companies.
- Forward suspicious emails as attachments to cwopa_spam@pa.gov for review by IT security staff.

Records with Personally Identifiable Information (social security number, date of birth, etc.) or other confidential data should never be handled in a home office unless an employee has specific permission to do so. Confidential records that are stored on personal computers or printed on home printers are stored within the hard drives of those devices and is vulnerable. If authorized to use such records outside the office, employees must ensure that they are available only to authorized individuals. The theft of such information can have catastrophic consequences for the individuals whose data is stolen, and the commonwealth—and employees—can face significant consequences as well.

If physical records need to be destroyed before an employee can return to their office, they should be shredded and not placed in regular recycling. Electronic files should be permanently deleted and not simply moved to a computer's recycle bin.

Commonwealth Information Technology Policies Relevant to Teleworking and Records Management

ITP-SEC000: Information Security Policy
ITP-SEC007: Minimum Standards for IDs, Passwords, and Multi-Factor Authentication
ITP-SEC015: Data Cleansing Policy
ITP-SEC019: Policy and Procedures for Protecting Commonwealth Electronic Data
ITP-SEC035: Mobile Device Security Policy

Other Resources

Best Practices for Cloud Computing Records Management Considerations (North Carolina Division of Archives and Records)
OneDrive for Business: Best Practices and Usage (North Carolina Division of Archives and Research)
E-records Guidelines (Pennsylvania State Archives)
Best Practices for Electronic File Folders (Pennsylvania State Archives)
Electronic File Naming Guide (Pennsylvania State Archives)
Saving Email Decision Guide (Pennsylvania State Archives)
Protecting PII: Telework Best Practices (U.S. Department of Homeland Security)
Telework Guidance: Security and IT (U.S. Office of Personnel Management)
Telework Best Practices (Pennsylvania Office of Administration)
PA Protecting Yourself Online Guide (Pennsylvania Office of the Governor)