

Microsoft 365: Best Practices and Usage

October 2021
Version 1.1



NC DEPARTMENT OF
NATURAL AND CULTURAL RESOURCES

Contents

Purpose	2
Technical Overview	2
Records Management Modules.....	2
SharePoint Online	3
OneDrive for Business.....	4
Tools Related to OneDrive for Business and SharePoint	4
Teams.....	4
Stream.....	5
Delve	5
Records Management in Office365	5
Access Restrictions.....	5
Audit Trails	5
File Naming	5
File Structuring.....	6
Retention and Disposition.....	6
Confidentiality.....	6
Records Destruction.....	7
Managing Records in OneDrive	8
Electronic Records Policy	9
Archival File Formats.....	9
Division of Responsibilities Between DIT and Records Agency	9
Conclusion.....	10

Purpose

Executive Agencies and the Department of Information Technology have purchased Microsoft's Office 365 (O365) subscription services. Office 365 designates subscription plans that include access to Office applications plus other productivity services available via cloud services. Two elements of this subscription available to state employees in North Carolina are OneDrive and SharePoint. Cloud services provide easy access, collaboration features, and flexibility to state employees; however it also presents unique records management challenges.

This document offers guidance and best practices in the following areas:

- A technical overview of OneDrive, SharePoint, and related applications
- Records management best practices for using OneDrive and SharePoint in your agency

Adherence with the recommendations laid out in this document will support more efficient document retrieval, mitigate the loss of public records due to inaccessibility or unscheduled erasure, and improve the agency's ability to respond to public records requests.

Technical Overview

The North Carolina Department of Information Technology (DIT) has purchased Microsoft Office 365 for use by DIT-supported state agencies. Office365 includes the latest version of Microsoft Office software (Word, Excel, PowerPoint) in the OneDrive for Business package so users can make changes to documents from different devices, even if they do not have the software locally installed.

Office 365 is managed at three levels: tenant, library, and team. The tenant level is the entire set of servers making up Office 365 and its associated features. It holds all the content for all state agencies using DIT's instance and is managed by NC DIT. The library is a container within a SharePoint site or Team that holds file folders and documents. It is managed by the SharePoint or Team administrator. A team is a group of individuals within the Teams tool that will be explained further below.

All information in Office 365 is stored remotely on servers owned by Microsoft and located in the continental United States. This concept of storing information in a remote location is often referred to as cloud storage. For more information on records management and cloud storage for North Carolina state agencies, please see *Cloud Computing and Public Records*, available at <https://archives.ncdcr.gov/government/digital-records/digital-records-policies-and-guidelines/best-practices-cloud-computing>.

Records Management Modules

Office 365 is a multi-faceted system that advertises several modules to assist customers in managing their files. These modules include:

- Audit
- Data loss prevention
- E-discovery
- Information protection
- Information governance
- Records management

These modules are options that must be turned on. In the DIT environment, the following have been activated:

- Audit

- Data loss prevention
- E-discovery (including legal hold)

In addition to these modules at the tenant level, there are other modules that can be deployed at other levels within DIT's instance. For example:

- Library Level
 - Information Management Policy Settings, such as setting retention rules
 - Information Rights Management (Information Protection), such as defining security classifications and encryption
- Teams Level
 - Archive

Please visit [Microsoft Office 365 documentation online](#) or contact DIT for more information on these modules and potential deployment options for your agency.

SharePoint Online

SharePoint Online is the “foundation” of many features in Microsoft 365, including Microsoft Teams and OneDrive for Business, all of which are used to store digital documents in a cloud environment. It serves as a collaboration tool that combines several functions, including: intranet, extranet, content management, document management, personal cloud, business intelligence, workflow management, and web content management. In addition, SharePoint provides central management, governance, and security controls for content management and collaboration.

SharePoint is a browser-based tool that provides communication and collaboration tools to improve productivity and efficiency in the government workforce. Within SharePoint users can store, track, and manage electronic documents and assets. The primary location for documents is a “document library,” which is designed to manage up to 30 million documents, videos, or images. These libraries can be accessed via sites, which can be set up independently in SharePoint, or nestled under a Team. These sites can contain up to 25 TB of content. If this size limit is reached, a new site must be requested.

Document libraries can be configured with retention policies by site owners, the designated individual within the agency who has full control privileges to the site. They may also be configured at the tenant level by requesting that a site be put on legal hold, which may impact the ability for end users to save, rename, delete, and list items on the site.

Additional tools include:

- Versioning — SharePoint allows some versioning of documents by allowing them to be “checked in” and “checked out” and will manage the versions of the document so that users are aware of the most up-to-date version.
- Collaboration — SharePoint enables users to collaborate in real time using the live collaboration and editing tools, thus reducing the need to generate and manage emails.
- Synchronized files — Because it is centrally hosted, SharePoint can synchronize files across devices.
- Rights Management — SharePoint site owners within each agency can set user permissions (i.e., read, write, modify, access).
- Search — SharePoint allows users to search across sites and configure the results to display information they wish to see—all, by format, by date—and allows the user to define how the results to be displayed in different ways—grid, detailed, filtered, etc.
- Updated software — In a hosted instance, the software is updated independent of users and users content and sites are upgraded automatically so that content is accessible regardless of the software used to originally create it.
- Ability to “tag” files — SharePoint provides tools to allow users to “tag” documents utilizing a taxonomy developed by the site users. The tagging feature makes it easier to search and retrieve documents.

OneDrive for Business

OneDrive for Business sits on a foundation consisting of SharePoint Online and uses many of the same functions found in SharePoint Online but does not have the same capability for configuration that SharePoint Online does. OneDrive is “online storage space in the cloud that’s provided for individual licensed users in an organization. Use it to help protect work files and access them across multiple devices. OneDrive lets you share files and collaborate on documents, and sync files to your computer.”¹ OneDrive is suitable for storing documents that are still in progress but are not quite ready for sharing or distribution.

OneDrive for Business is similar to other cloud storage and sync options such as Dropbox, iCloud, and Google Drive. However, OneDrive for Business is an approved tool for use with state information and provides employees the ability to access from multiple devices. Unlike Dropbox, iCloud, and Google Drive, OneDrive for Business access is authenticated and authorized by the employee’s NCID account; therefore, any document stored there will become inaccessible after an employee separates from the agency. OneDrive for Business can store multiple file formats including images and video, as well as Microsoft Office formats. OneDrive for Business is compatible across multiple operating platforms and browsers, including Apple iOS, Android, and Linux. **Of major concern, however, is that once an employee leaves an agency or terminates employment with the state, information stored on their OneDrive for Business will become inaccessible and unrecoverable, since the account will be closed. Policies should be in place for agencies for the management of these records (for further guidance, see the section below on managing records in OneDrive).**

Tools Related to OneDrive for Business and SharePoint

There are several tools within Office365 that interact with OneDrive for Business and SharePoint. It is important to remember that all materials shared in these tools are subject to the public records law and should therefore be used in a manner in accordance with the below guidelines.

Teams

Microsoft Teams is an instant messaging and remote meeting tool that is built over SharePoint (for file and content storage) and Exchange (for chat). Communication can be done in Teams using channels or private chats. Channels are general messaging boards with a targeted focus, such as a specific division or section, while private chats are between individuals or smaller groups. Generally, channels are good for general information sharing, whereas private chats allow for more targeted conversations. Teams stores chats and shared files in OneDrive for Business and SharePoint, depending on the nature of the interaction; private chats are stored in the user’s OneDrive, while Team channels are stored in SharePoint. The conversation history and Teams chats are recorded in users’ email inboxes and are discoverable in eDiscovery by eDiscovery managers, depending on the agency parameters. Space for content in Teams by default is 1TB but can be expanded to 25TB. If this size limit is reached, a new team must be requested.

Teams contain multiple productivity tools including:

- Focused “channels” that team owners can create for their teams that would contain chats and content based on a specific subject, tasks or project.
- Chats
 - Team chats – open to the entire team
 - Private chats – not connected to a specific team and private between those you are chatting with.
- Planner
- OneNote
- Various “tabs” such as PowerBI, and “webpage” tabs
- Calendar [for scheduling Team meetings, tied to your Outlook [Exchange] Calendar]

¹OneDrive Service Description, retrieved 9/9/2021, <https://docs.microsoft.com/en-us/office365/servicedescriptions/onedrive-for-business-service-description?redirectedfrom=MSDN>

- Channel Calendar [for setting up meetings or tracking events, etc. in channels. Meetings are tied to your Outlook calendar
- Files – tied directly to the document libraries where content is stored. Each “channel” has a “file” tab

Stream

Microsoft Stream is a video sharing software. It stores recorded Teams video meetings and calls, as well as uploading and sharing videos, and live streaming events. Videos shared in Stream are stored in SharePoint and OneDrive. Stream also creates transcriptions for discovery of video in eDiscovery. Storage of Stream videos is based on DIT-set retention periods; agencies should work with DIT to determine retention rules of videos they generate.

Delve

Microsoft Delve is a layer on SharePoint that operates much like Pinterest, based on the search index in SharePoint. The graphic user interface (GUI) shows the user all of the files that they have access to, and displays how many times the user has viewed the document. It is a secure access layer that will not change existing permissions of a file set by the file’s owner.

Records Management in Office365

Access Restrictions

Access rights to SharePoint and OneDrive and individual locations in SharePoint and OneDrive should be managed by IT and assigned by a supervising authority within the agency to prevent unauthorized viewing of records. Access to confidential and non-confidential records on SharePoint and OneDrive should be appropriately managed and folders and file structures should reflect any applicable access restrictions. Access passwords to SharePoint and OneDrive should be securely kept outside of SharePoint and OneDrive.

Audit Trails

It is recommended that documentation be created pertaining to who has read and/or write permission to files maintained by the agency in SharePoint and OneDrive. Default settings for both SharePoint and OneDrive contain metadata concerning who created and/or modified records and when.

File Naming

Naming conventions on SharePoint and OneDrive should follow the [Best Practice For File Naming](#) guidance published by the NC Department of Natural and Cultural Resources.

The Best Practice guide recommends the following formatting:

- Avoid special characters
- Use underscores instead of periods or spaces
- Be brief
- The file name should include all necessary descriptive information independent of where it is stored
- Include dates and format them consistently
- Include a version number
- Be consistent

The Best Practice guidance provides additional detail concerning these recommendations.

To recap, file naming should be consistent regardless of whether records are stored locally, on a server or on SharePoint or OneDrive.

File Structuring

Records stored in SharePoint must be easily navigable by other users, present and future. As such, structuring of the folders and sub-folders should be done in a logical manner.

Logical file structuring can provide context to records. The [Functional Schedule](#) can provide guidance on how file structures may be patterned by using the functions, sub-functions, and record types as delineated in the schedule as guides. Folder naming should follow the same guidelines used for file naming found in the [Best Practice For File Naming](#) guidance published by the NC Department of Natural and Cultural Resources.

Regardless of how users structure their folders in SharePoint they should avoid creating hierarchies deeper than four or five folders. This can create problems when migrating or moving data. Files may also become unreadable to the operating system and lost in migration if nested too deeply within a hierarchy.

Retention and Disposition

Users of SharePoint and OneDrive must be aware that records stored on either platform are subject to the appropriate retention defined by the [Functional Schedule](#). It is the agency's responsibility to ensure that records stored in these platforms are retained and accessible until the records disposition instructions are met. Having electronic records policies in place can provide a framework for records with long-term and/or permanent retention (See below for details on electronic records policies).

Confidentiality

Confidential data includes information that if accessed by unauthorized entities could cause personal or institutional financial loss or constitute a violation of statute, act, or law. Below is a non-exhaustive list of records that are subject to confidentiality restrictions:

- Personal identifiable information such as library records that identifies a person as having requested or obtained specific materials or service²
- Confidential communications by legal counsel to public board or agency, state tax information, public enterprise billing information, or records associated with the Address Confidentiality Program, as well as documents related to the federal government's process to determine closure or realignment of military installations³
- Trade secrets or information disclosed or "furnished to a public agency in connection with the owner's performance of a public contract or in connection with a bid, application, proposal"⁴
- Login/password credentials⁵
- Those that reveal "the electronically captured image of an individual's signature date of birth, driver's license number or a portion of an individual's social security number"⁶

² Confidentiality of library user records. (1985). Retrieved September 15, 2021, from <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=125>

³ Confidential Communications by Legal Counsel to Public Board or Agency; State Tax Information; Public Enterprise Billing Information; Address Confidentiality Program Information. Chapter 132. Public Records. North Carolina General Assembly, 1995. Retrieved September 15, 2021, from <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132>

⁴ Confidential Communications by Legal Counsel to Public Board or Agency; State Tax Information; Public Enterprise Billing Information; Address Confidentiality Program Information. Chapter 132. Public Records. North Carolina General Assembly, 1995. Retrieved September 15, 2021, from <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132>

⁵ Inspection and Examination of Public Records. (2014). Retrieved September 15, 2021, from <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132>

⁶ § 132-1.2. Confidential information. (2014). Retrieved September 15, 2021, from <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132>

- Those that reveal the seal of a licensed design professional⁷
- State Employee Personnel files (with the exception of certain information that can be disclosed).⁸
- Protected health information (PHI) in any form or medium created or received by a health care provider, health plan, employer or clearinghouse. PHI is defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as health information “that identifies the individual” or “with respect to which there is a reasonable basis to believe the information can be used to identify the individual.”⁹ The Public Health Law of North Carolina also stipulates the confidentiality of “privileged patient medical information” in the possession of DHHS or local health departments.¹⁰
- Student records protected by the Family Educational Rights and Privacy Act of 1974 (FERPA).¹¹

Confidential records stored on SharePoint and OneDrive should use the following safeguards.

- Password protection
- Encryption
- The use of Security Alerts whenever a file is accessed.
- The use of a confidential tag in the file’s naming structure.

DIT can provide guidance on how to specifically enable password protection, encryption and security alerts in SharePoint and OneDrive.

Please note that if encrypted or password protected documents are eligible for transfer to the State Archives for permanent retention, they will need to be decrypted and accessible at the time of transfer. See [Digital File Transfer Guidelines](#) for more information.

Records Destruction

Agencies should maintain an inventory of all of their records and where their records are stored. It is an Agency’s responsibility to properly purge all records that have met retention requirements, including copies stored on SharePoint and OneDrive. Prior to destruction, agencies should check that they are using the current, approved schedule by checking the posted [functional schedule online](#), consulting your agency’s [Chief Records Office](#), and/or contacting the [records analyst assigned to your agency](#). When digital records are deleted in Microsoft 365, the content is stored in the end user recycle bin for 30 days. Subsequently, tenant-level recycle bins store the deleted content for a total of 93 days after which the files cannot be recovered.

⁷ § 132-1.2. Confidential information. (2014). Retrieved September 15, 2021, from <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132>

⁸ Chapter 126. North Carolina Human Resources Act. (2014). Retrieved September 15, 2021, from <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=126>

⁹ HIPAA ‘Protected Health Information’: What Does PHI Include? (2015). Retrieved September 15, 2021, from <https://www.hipaa.com/2009/09/01/hipaa-protected-health-information-what-does-phi-include/>

¹⁰ Chapter 130A. Public Health. § 130A-12. Access to Health Information. North Carolina General Assembly, 1983. Retrieved September 15, 2021, from <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=130A>

¹¹ “Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g; 34 CFR Part 99.” U.S. Department of Education. U.S. Department of Education, 26 June 2015. Retrieved September 15, 2021, from <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Records that have met their retention requirements should be destroyed in accordance with the [North Carolina Administrative Code](#). North Carolina Administrative Code 07 NCAC 04M .0510 provides a description of the authorized methods for the destruction of public records in North Carolina. It states:

“ . . . (b) When used in an approved records retention and disposition schedule, the provision that electronic records are to be destroyed means that the data and metadata are to be overwritten, deleted, and unlinked so the data and metadata may not be practicably reconstructed.













(c) When used in an approved records retention and disposition schedule, the provision that confidential records of any format are to be destroyed means the data, metadata, and physical media are to be destroyed in such a manner that the information cannot be read or reconstructed under any means.”

All agencies should maintain logs of their destructions in their Records Management file.

Confidential records must be destroyed in such a manner that the records cannot be practicably read or reconstructed.

Managing Records in OneDrive

Unlike SharePoint, OneDrive for Business accounts are tied specifically to an individual employee’s authenticated authorized account. OneDrive accounts and the files stored within may or may not be generally accessible to other employees or IT professionals, depending on whether the records are shared or private. Some Microsoft 365 content is automatically saved in a user’s OneDrive such as Teams chat files, Whiteboards, wikis, and meeting recordings hosted by the user. Employees are responsible for managing their records appropriately and following agency records management policies.

 RATOM	July 17, 2020	Patrick-Burns, Jamie A	2 items	 Shared
 Transition_documentation	July 2, 2020	Patrick-Burns, Jamie A	6 items	 Shared
 Microsoft Teams Chat Files	June 10, 2020	Patrick-Burns, Jamie A	19 items	Private
 Digital_Records_AXAEM	June 5, 2020	Patrick-Burns, Jamie A	2 items	 Shared
 Move_db_samples	May 29, 2020	Patrick-Burns, Jamie A	9 items	 Shared
 AccessCopies	April 13, 2020	Patrick-Burns, Jamie A	4 items	 Shared
 Attachments	March 16, 2020	Patrick-Burns, Jamie A	39 items	Private

Example of Microsoft 365 automatically stored content in OneDrive. Each user’s folders may be different based on the applications they use.

It is crucial to note that OneDrive for Business is tied to the account activated for a state agency employee. In order for this account to be created, the employee must be authenticated and authorized. For Microsoft services, the account is an employee’s e-mail address and NCID password. Because it is the entire email address, each agency has a specific domain within OneDrive for Business; therefore, stored documents will not transfer when an employee moves from one state agency to another. When an employee leaves an agency (even if transferring to another agency), the employee must review documents and files in OneDrive for Business. When a user account is eventually deleted, so is the content associated with that OneDrive for Business account. An employee’s OneDrive account will be retained for five years after separation, during which time the contents will be available to the user’s supervisor and any other designated users, as well as eDiscovery. After that time, any records that a scheduled for permanent and/or archival disposition

must be stored elsewhere. For this reason, Human Resource Directors and employees' supervisors must ensure that migrating files out of OneDrive for Business becomes part of the mandatory offboarding process when an employee leaves the agency. Discuss storage options for records with a permanent and/or archival disposition with your supervisor and/or your agency's IT professionals.

Information Technology staff are a critical support piece for records management. DNCR encourages agency management to communicate their storage needs to IT in order to properly manage the records and ensure the appropriate management of information assets. DNCR strongly recommends that agencies form an Information Governance Committee to set policies regarding how and where records are stored and managed. At a minimum, the members of that committee should consist of information technology staff, the chief records officer, the records manager (if applicable), as well as a high level executive sponsor or manager.

Electronic Records Policy

All state agencies should have an Electronic Records Policy in place. This may be done as an agency-wide policy or be broken up into separate policies concerning specific divisions, sections, or other organizational structure. The Electronic Records Policy is designed to be used as a self-evaluation tool to ensure that electronic records produced by state agencies are able to be retained for the designated retention period and are created, reproduced, and otherwise managed in accordance with guidance produced by the Department of Natural and Cultural Resources. Agencies should address SharePoint and OneDrive usage in their respective policies.

Archival File Formats

While SharePoint and other Office 365 programs can store a variety of file formats, not all formats are considered archival. File formats are considered archival when those formats meet the minimum requirements for long-term retention, including documentation, wide adoption, transparency, self-containment, and use within the archival community.

Any file with a permanent or long-term retention requirement should be saved in an archival file format. You may find a list of those recommended formats in [File Format Guidelines for Management and Long-Term Retention of Electronic Records](#).

Division of Responsibilities Between DIT and Records Agency

Managing long-term records within SharePoint requires an active partnership between the records custodial agency and the Department of Information Technology (DIT). DIT is NOT the records custodian for records stored exclusively in SharePoint.

The custodial agency should still fulfill the following roles:

- Correspond with DIT to obtain audit trails on a regular basis to track any changes to long-term records
- Arrange records in the agency's SharePoint instance according to best practices for files and filing as laid out elsewhere in this document
- Ensure that individual employee records stored in OneDrive are transferred to SharePoint prior to the employee separation or supervisor assigned temporary access must retrieve records in OneDrive immediately after employee separates
- Respond to litigation or audits that require access to a record stored in SharePoint
- Fulfill public records requests for records stored in SharePoint
- Delete records from SharePoint once the records have met their required retention period (if applicable) and document destructions in a destruction log
- Ensure that agency employees do not delete long-term records before retention is met

- Ensure that employees do not open and edit inactive records without due cause. Editing inactive records can restart the retention clock for some long-term records.

DIT will fulfill the following roles:

- Act as administrator and backend manager for Office 365
- Manage the following back-end modules:
 - Audit
 - Data loss prevention
 - E-discovery (including legal hold)
- Retrieve files deleted erroneously, if an automated backup version of the file is available
- Retrieve chats from Teams if no longer accessible by the front-end user
- Technical troubleshooting for general Office 365 issues

Conclusion

- Office 365 offers cloud-based productivity tools such as Microsoft Office suite, SharePoint, and OneDrive. Materials/files can be accessed across multiple devices with ease and security.
- O365 is managed at the tenant, library, and team levels. NC DIT has activated audit, data loss prevention, and eDiscovery functionality, while agency SharePoint administrators are responsible for collaborating with IT to configure rights management and setting retention policies for content.
- Digital records require active management by the records creators, and records management best practices are to be observed and documented in an electronic records policy. Each agency is responsible for managing permissions, protecting confidential records, documenting audits, planning file naming and structure, and following retention and destruction guidance.
- Employees' OneDrive for Business is not intended for permanent storage of public records.

This document supersedes One Drive for Business: Best Practices and Usage, April 2020, Version 2.0.