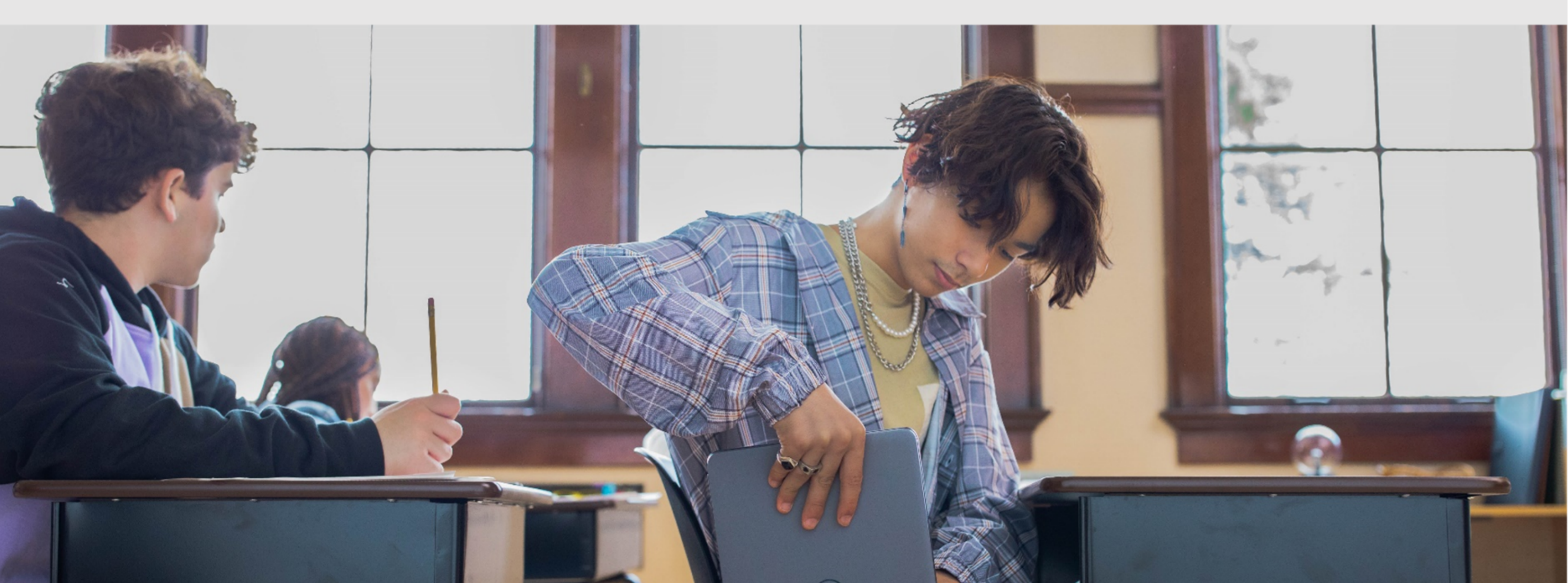
# Best practices for information lifecycle and storage management in education

July 2023

# Contents



# How to use this document

With the shift away from unlimited free storage, many IT leaders at educational institutions are taking a closer look at their organizations' information lifecycle and storage management practices. This paper provides holistic guidance for refining information lifecycle and storage management approaches at both K-12 and higher education institutions to help leaders ensure cost efficiency and protect information institution-wide.

**Terminology:** All K-12 and higher education institutions are collectively referred to as "institutions."

# The importance of information lifecycle and storage management

Information lies at the heart of education—it's the raw material that students, teachers, and faculty use to fuel learning and innovation. As hybrid learning and work have become more prevalent, the sheer volume and diversity of information stored digitally has skyrocketed—and while this presents institutions with exciting opportunities, it also introduces new challenges. It can be difficult to maintain security, compliance, and appropriate access for this information, all while striking a balance between academic freedom and proper management and control.

Moreover, given the historical trend of free, unlimited storage, many institutions have grown accustomed to letting their users store anything and everything in their systems, including content that may not be necessary or require frequent access. As cloud service providers begin to set limits on storage, this approach can have significant effects on storage costs, information security, and more.

But there's also much to gain from well-developed information lifecycle and storage management practices. To start, institutions can reduce the risk of a security breach by managing information's governance, lifecycle, and security and access policies. With the move to the cloud, the amount of files, data, and inactive accounts have proliferated over time, and many institutions have used up more and more cloud storage without a formal plan for deleting or archiving information. This widens the attack surface and puts institutions and their students at increased risk for data breaches. Today, education is the most-targeted industry by cybercrime, with K-12 receiving over 80% of workplace malware attacks.

In addition, stored files that are no longer in use impact our carbon footprint. Over half of all data stored by organizations does not serve a useful purpose, and storage of this "dark" data takes up space on servers, resulting in increased electricity consumption and the release of an estimated 6.4 million tons of CO2 in 2020 alone.[1] Because Microsoft is committed to both the security and privacy of school and student data as well as reducing our collective carbon footprint, our datacenters are built with the highest environmental standards in mind—and with this change, education customers can help do their part.

[1] Veritas, April 2020 https://www.veritas.com/news-releases/2020-04-21-veritas-technologies-projects-dark-data-to-waste-up-to-6-4-m-tons-of-carbon-dioxide-this-year

# Understanding your storage options

IT leaders have many considerations when setting out on their storage journey, but they should first determine which storage solutions are appropriate for the various kinds of information held by their institutions. Because Microsoft 365 and Azure are intended for different use cases and have distinct cost implications, it's critical to consider which solutions are best for various information types to reduce costs and enable better governance over information.

## Microsoft 365 storage

Microsoft 365 is intended to facilitate small file storage and collaboration. This includes files used by students, faculty, and staff that require frequent access or short-term storage (for example, one academic year.) Microsoft 365 storage is not intended for large datasets (such as high volumes of research data), archival, or infrequently accessed information. It includes storage across OneDrive, SharePoint, and Exchange mailboxes:

- OneDrive is designed for storing files that will be accessed by the document owner or shared with a few others through a link. For instance, students may store assignments in their OneDrive before submitting it to an instructor through the institution's learning management system (LMS) or Assignments in Teams.
- SharePoint is designed for storing files that will be accessed by and collaborated on by many users, and it can be used with LMS solutions like Canvas or Blackboard. An example of a file that might be stored in SharePoint is a group PowerPoint presentation, where a team of students may need to constantly access and edit the file simultaneously. Because SharePoint is also the backend for Microsoft Teams, files sent between users on this platform will automatically be stored in SharePoint.
- Exchange is the backend for Outlook mailboxes. Storing files in Outlook and Exchange is not recommended, but users tend to send emails with file attachments. Because of this, we advise you to guide your users to share links to files stored in SharePoint or OneDrive via email instead of attaching copies of the files themselves.

Beginning August 1, 2024 (or at a school's next contract renewal) every school has a 100TB base storage capacity. Microsoft 365 and Office 365 A3 and A5 paid user licenses add 50GB or 100GB respectively to the pool of storage. In addition, schools can purchase additional pooled storage in 10TB increments for $300 estimated retail USD monthly to add to the tenant pool.

## Microsoft Azure storage

Microsoft Azure is intended for files and data that are either very large, less frequently accessed, or require longer term archival, such as research datasets or large workloads. Azure access tiers include the hot tier for storing data that's frequently accessed, the cool and cold (now in preview) tiers for data that's infrequently accessed, and the archive tier for data that's rarely accessed.

With Azure, there's an inherent tradeoff between cost and ease of access. Hot storage is more costly but easier to access, while cold storage is less expensive but less readily accessible. The below table details the available Azure storage tiers, ranked by cost, with guidance about when each tier should be used. (Please note that the prices are sample pricing from the Azure East US region.)

| Azure Service | Cost per month per 10 TB *(Sample pricing as of June 2023—Azure East US region)* | Notes | Scenarios |
|---|---|---|---|
| **Azure Blob Archive** | $11.64 | Cost excludes retrieval charges | Rarely accessed unstructured data, such as data that must be kept for compliance reasons but is not expected to be accessed again. An example would be raw research data from a past project where the findings have already been published. |
| **Azure Blob Cool** | $155.65 | Cost includes only a limited number of transactions | Infrequently accessed unstructured data that should still be available immediately if needed. |
| **Azure Blob Hot** | $212.99 | Cost includes only a limited number of transactions | Frequently accessed data that needs to be accessed by specific groups, including large groups. Examples include active media viewed by the community (leadership addresses, sporting events), actively processed research data, and publicly available data sets. |
| **OneLake** | $216.45 | Additional charges may be incurred for Fabric licenses | Value-added service for data lake workloads based on Azure Blob storage. |
| **Azure Files Cool** | $221.12 | Pricing for one-year reservation and includes only a limited number of transactions | Backups, intermediate output, research data archival to be accessed using SMB (from Windows clients) or NFS (from Linux clients) protocols. |
| **Microsoft 365 (August 2024)** | $300.00 | First 100 TB included | User and team productivity and collaboration, such as Office files and Teams meetings. |
| **Azure Files Tx Optimized** | $614.43 | | Replaces on-premises SMB or NFS file shares with 1,000+ users actively accessing. |
| **Elastic SAN** | $819.20 | | Value-added service for specialized workloads requiring high transaction rates and mounting remote storage over iSCSI. Examples include databases and enterprise systems, such as SIS and LMS. |
| **Azure Media Services** | Dependent on service and volume processed | | Value-added service for indexing, converting, and streaming media files. |

## Education storage use cases

Now that we've given an overview of Microsoft storage options, the rest of this paper will provide best practices for use cases across three key areas:

1. **Teaching and learning information,** which includes information and files created and used by students and faculty in Microsoft 365, such as assignments, curricula, or extracurricular documents like sports and club information
2. **Research information,** which includes information used and created in research, such as streaming data, simulations, genomics data, and more
3. **Administrative information,** which includes information and files managed by institutional staff, such as academic transcripts, health records, and financial information

We recognize that the lines between information types are muddled, but we've defined these categories to organize the following discussion. Importantly, this guidance is also limited to information for which Microsoft storage solutions are applicable. It will not comprehensively address all information types present at the typical educational institution.

Finally, this paper does not need to be followed step-by-step—you can jump to the sections that most suit your scenarios. Explore the additional resources at the end of the document to see all the services available for managing your institution's information lifecycle and storage practices.

# 1. Teaching and learning information

Teaching and learning information encompasses the documents, files, and information created and stored by an institution's students, faculty, and staff in their school OneDrive, SharePoint, and Exchange accounts (such as assignments, school curriculum, or extracurricular files like sports or club information.) This section will cover how to:

- **Encourage appropriate use** to foster a safe, private, productive learning environment
- **Set policies and manage lifecycles** to optimize students' and educators' storage in Microsoft 365

## Encourage appropriate use

It can be challenging to ensure that students, educators, and staff follow best practices for storage. They may house personal files on school accounts, hang onto unnecessary files, store content that violates institutional policy, or use cloud storage solutions your institution doesn't condone. And educators have the additional challenge of helping to ensure that grades, assessment results, and other sensitive information about students is kept private.

**Communicate good storage habits.** To help you share storage best practices with students and educators, we've created an End User Guide, which includes steps to help maintain storage hygiene. This can be sent to new cohorts of students (such as on the first day of class or during freshman orientation) or newly hired educators and staff. You may consider adding to this document, or merging it with your existing guidance, to instruct users about your institution's unique policies and code of conduct.

**Prevent inappropriate sharing of sensitive content.** To help prevent the unauthorized sharing of sensitive data—such as feedback written by instructors about students—you can set up Information Rights Management (IRM), available in Microsoft 365 A5 suites, in the SharePoint admin center. This uses encryption, identity, and authorization policies to safeguard files and emails across devices, ensuring that authorized individuals inside and outside your institution can access data, while preventing access to unauthorized individuals. Please note that before you can IRM-protect SharePoint lists and libraries, you must first activate Azure Rights Management for your institution.

To mitigate the sharing of inappropriate content, there's Microsoft Purview Communication Compliance, available in Microsoft 365 A5 suites, which helps you detect and address inappropriate or potentially inappropriate communications like threatening language. Using both pre-defined and custom policies, you can scan communications inside and outside your institution for possible violations. Reviewers can then investigate email, Microsoft Teams, and other applications with this content and take action accordingly.

## Set policies and manage lifecycles

From film students uploading raw footage to English majors writing essays that only use a handful of kilobytes, we know your user base has a diverse range of storage needs. For detailed guidance about how to get insight into storage usage—including how to run reports in OneDrive, SharePoint, and Exchange—and how to customize storage limits for each user or user group, consult our Storage Guidance eBook.

Below are a few other tips and tricks about managing file and user lifecycles.

**Manage file lifecycles.** For SharePoint and OneDrive sites, one way to determine whether a site can be deleted is to reference recent activity. As an admin, you can identify the largest sites in the admin centers for SharePoint and OneDrive. If you find large sites with no recent activity, you can then contact the site owner to determine whether the data should be kept for compliance purposes or otherwise—and if not, you can assess whether the site can be deleted. If it's not being used but must be kept for compliance (such as a federal or state regulation governing how long academic information must be retained), it can be moved to Azure blob storage. From there, its version history, access settings, and more would need to be maintained.

To help automate compliance, you can also set retention policies to determine how long sites and files should be kept live, as well as how long they should be stored after archival. We recommend tagging sites by their type and importance and assigning retention periods, which can be accomplished with a records management solution like Microsoft Purview. For files, you can set retention policies to hold them only for a certain amount of time to periodically free up storage space and eliminate the need for manual deletion. To do this in OneDrive, SharePoint, and Exchange, you'll need to decide whether you'd like to create adaptive or static policies, and then you can create a retention policy for those locations.

**Manage user lifecycles.** To manage and delete inactive users—such as alumni, visiting professors, transfer students, and former employees—you can start by leveraging reports in Microsoft Graph and Microsoft Entra ID Governance. You can gain visibility into the last activity dates of users, and then delete inactive users in bulk and set group expiration policies. For alumni specifically, it's important to determine how much storage they will be allotted post-graduation (e.g., 15 GB). You can then communicate this limit to them and give advice on how to reduce their storage.

# 2. Research information

Research information can be difficult to manage due to its varied data types, high volumes, and diverse user needs. It's not enough to give all researchers the same amount and type of storage space, since their needs will vary according to the type of information they have—covering a wide gamut including basic text files, large audio and video captures, vector graphics, bibliographies, programming files, simulations or models, and unique filetypes like FASTQ, BAM, and JSON for genomics. This section will cover how to…

- **Allocate storage based on researcher's needs**, including nuances around structured vs. unstructured data
- **Adapt to compliance and grant requirements** to simplify adherence to both internal and external regulations
- **Enable external file sharing** for collaboration with researchers from other institutions

## Allocate storage based on researchers' needs

It goes without saying that different kinds of research have different storage considerations. Faculty working with large amounts of unstructured or semi-structured streaming data will need a lot of storage that can accommodate unstructured data types, whereas researchers working with databases and other structured data may need warehouses with specific schema.

**Use hot, cool, cold, and archive access tiers.** In Azure Storage, you can organize blob data based on how frequently it will be accessed and how long it will be retained. As mentioned above, Azure Storage offers access tiers that include a hot tier, cool tier, cold tier (now in preview), and an archive tier. In academic research, hot storage is ideal for active research projects such as recent experimental results, survey responses, live sensor data, drafts of manuscripts, and frequently accessed datasets used in machine learning models, large-scale simulations, or real-time monitoring systems. Cold storage is better for finalized, published research data, older datasets, and reports no longer in use, and archives mandated by funding agencies or regulatory bodies, as well as backup and disaster recovery.

**Choose the right solution for your scenario.** Below is a brief overview of a few key Azure storage solutions available for both structured and unstructured data. For a more complete breakdown, visit this page.

- Azure Blob Storage is object storage optimized for massive amounts of unstructured data. Blob Storage allows you to store files for distributed access; data for backup and restore, disaster recovery, and archiving; and data for analysis. It's highly scalable, and users can access objects in Blob Storage via HTTP/HTTPS from anywhere in the world to facilitate collaboration between researchers. Blob Storage is also integrated with Azure Managed Lustre (preview), an open-source parallel file system designed to scale to massive storage sizes while providing high-performance throughput. When integrating with Blob Storage, you can import files from a blob container and export changed data back to Blob Storage when finished. Beyond integration with Blob Storage, it can help you provision, configure, and manage your Lustre file system—using the Azure portal, you can quickly deploy a Lustre file system in the size you need, helping you allocate the right amount of storage for unstructured research data. This is particularly helpful for researchers working with high-performance computing and data-intensive applications.

- Azure Files enables you to set up highly available network file shares. Multiple virtual machines can share the same files with both read and write access. You can access the files from anywhere in the world using a URL that points to the file and includes a shared access signature (SAS) token. You can generate SAS tokens; they allow specific access to a private asset for a specific amount of time. Azure Files integrates seamlessly with various data science tools like Azure Machine Learning and Azure Databricks, which can be useful for many researchers.
- Azure NetApp Files is enterprise files storage powered by NetApp. This solution makes it easy to migrate and run complex, file-based applications with no code change.
- OneLake is a single, unified, logical data lake for your whole organization, and as such it's designed to act as a single place for all your research data. Using OneLake, you can address data siloes while preserving access controls—making it an ideal place to store sensitive research data and other types of protected data, such as student or donor information.

**Scale high-performance computing workloads.** For both structured and unstructured workloads, you can expedite access to data using Azure HPC Cache and bring the scalability of the cloud to research data. You can use it even if your data is stored across WAN links, and you can launch and monitor it from the Azure portal for ease of management. Though there are many applications for HPC Cache, one example is life sciences. If a research institution wants to port its genomics analytics workflows, for instance, they could shift these workflows into Azure using HPC Cache with no client-side changes due to HPC Cache's POSIX file access, helping reduce the burden on administrators while easing access for end users.

## Adapt to compliance and grant requirements

It's also critical for researchers to comply with internal and external policies. Common governmental regulations like ISO 27001, NIST, HIPAA, and GDPR require identifying, classifying, and securing relevant information, especially if it's stored across systems or in inappropriate locations. In addition, compliance with grant requirements is essential to obtain research funding, and it's also crucial to keep up with standards implemented by institutional review boards (IRBs) to protect research subjects. With so many regulations and considerations, maintaining compliance can be a challenge, but the guidance below can help streamline the process.

**Set up a trusted research environment.** Using Azure Trusted Research Environments (TREs), you can enable researchers to work with sensitive datasets. Azure TRE is an accelerator that helps you build out trusted research environments on Azure, allowing users to set up and configure secure workspaces and tooling without IT teams. Along the same lines, the Azure Secure Research Enclave provides a reference architecture for a remotely accessible environment that allows researchers to collaborate as securely as possible on restricted datasets. If needed, it can support the use of analytical tools like Azure Machine Learning.

In Azure, you can take advantage of more than 100 compliance certifications, including over 50 specific to global regions and countries.

**Scan and classify assets across your data estate.** For data stored in Azure, you can use various Microsoft Purview data governance solutions to help you manage your on-premises, multi-cloud, and software-as-a-service (SaaS) data. First, you can automate data discovery with Microsoft Purview Data Map, which enables you to scan and classify assets across your data estate. It works by capturing metadata about enterprise data in analytics and operating systems both on-premises and in the cloud. It then connects it to apps like Data Catalog—which helps you find relevant data using a search—and Data Estate Insights, which provides high-level insights into governance gaps. For sharing data as securely as possible, there's Data Sharing, and for setting access policies you can use the Data Policy app. There's also Microsoft Entra ID Governance, which allows you to set conditional access policies when individuals leave or join an organization to set limits on which users can access sensitive data.

**Tag and encrypt information.** Microsoft Purview Information Protection provides advanced information protection capabilities, including data classification, labeling, and encryption to help keep your institution's information safe and compliant. It allows admins to classify sensitive research data and apply security policies to enable compliance with internal and government regulations, and it facilitates secure sharing and collaboration while maintaining control over data access and usage. You can create custom classification labels—such as "Confidential" or "Publicly Shareable"—representing different sensitivity levels determined by compliance regulations, ethical considerations, or any institutional requirements. In addition, Microsoft Entra ID Governance's identity lifecycle capability can help you manage digital identities representing people, organizations, applications, or devices to meet various access needs and permissions for sensitive data.

**Classify and retain research data in Microsoft 365 applications.** Using Microsoft Purview Data Lifecycle Management, you can automatically classify and retain research data based on predefined policies for information stored in Microsoft 365 apps. The solution offers intelligent data classification and tagging capabilities to help your institution identify and manage sensitive information more effectively, and it also assists in meeting regulatory requirements by implementing data retention and deletion policies.

**Identify and tag sensitive information in Microsoft 365 applications.** For information within Microsoft 365 applications, Microsoft 365 A3 and A5 licenses also allow you to automatically classify and label sensitive content. You can apply sensitivity labels, retention labels, and sensitive information type classification, and you can then monitor tagged information across your tenant. Before you create any new policies, the zero-change management capability will scan your sensitive and labeled content to ensure you can see the impact of any changes on your information before implementing them.

**Retain and version research data in Azure.** To manage versions of Azure blob data, you can use Azure Blob versioning to automatically retain previous versions of an object and help you recover data if it's inappropriately modified or deleted. You can also use it to restore containers, blobs, snapshots, or versions that have been deleted. For research data that is no longer being accessed but must be retained for compliance purposes, the immutable storage capability for Azure Blob Storage enables you to store data in a WORM state (write once, read many). When in this state, data can't be modified or deleted for a specified interval, which protects it from overwrites and deletes while still allowing objects to be read and created. All Azure blob access tiers (hot, cool, cold, and archive) support immutable storage, helping you keep your data as secure as possible wherever it's stored.

## Enable secure external file sharing

Another major challenge we've seen our users face is in managing access to research information. It's difficult to keep files and data secure while ensuring trusted users like internal and external researchers can share and access it, especially if it's stored in third-party systems or between institutions.

**Encrypt data and apply access controls to share information more securely.** You can help ensure shared files are secure with Azure Data Share, which allows for data to be shared securely through encrypted connections and access controls. You can set granular permissions to control who can access, view, or modify the shared data, and you can define sharing policies to enforce compliance with regulations, retention policies, and data privacy requirements. It also works seamlessly with other Azure services, such as Azure Blob Storage and Azure Data Lake Storage, making it easy to share large amounts of unstructured data in various locations.

To ensure only trusted individuals are able to access sensitive information, there's also risk-based Conditional Access and Identity Protection capabilities in Entra ID Governance, available with Entra ID Premium P2 licenses. Organizations can create risk-based Conditional Access policies according to two risk conditions—*Sign-in risk* and *User risk*—and then choose an access control method, such as multifactor authentication. Once applied, during each sign-in Identity Protection will analyze hundreds of signals in real-time to evaluate risk level, and it will then send the detected risk to Conditional Access which will apply risk-based policies.

Entra Premium P2 licenses also include Privileged Identity Management. This capability can help institutions minimize the number of people who have access to secure information to reduce the chance of a non-permitted individual gaining access or permitted users inadvertently modifying sensitive resources. It works by providing time-based and approval-based role activation, such as time-bound access, multifactor identification, notifications to administrators, and more.

**Set up highly available network file shares.** Using Azure Files' fully managed file shares, you can mount file shares concurrently by cloud or on-premises deployments, using industry-standard Server Message Block (SMB) protocol, Network File System (NFS) protocol, and Azure Files REST API. SMB Azure file shares are accessible from Windows, Linux, and macOS clients, and can be cached on Windows servers with Azure File Sync for fast access near where the data is being used.

# 3. Administrative information

Administrative information includes information and files created or handled by institutional staff, often containing sensitive data like transcripts, personally identifiable information (PII), financial information, or student health records. Beyond sensitive data from students and faculty, administrative information also encompasses a broad range of institutional data such as building plans, maintenance records, infrastructure details, budgeting and financial planning documents, accreditation records, strategic plans, and much more. This section will focus on the management of sensitive information, including how to:

- **Manage workload and mailbox retention** to maintain basic data hygiene across administrative information
- **Classify and protect sensitive items to** increase security and safety across your institution
- **Manage legal holds** for information where retention is legally required

## Manage workload and mailbox retention

**Establish a lifecycle management baseline.** First, it's important to establish a baseline level of lifecycle management across your workloads and mailboxes. In addition to helping you meet compliance and regulatory requirements, this reduces your institution's attack surface and helps you manage risk and liability. This baseline level of governance can be accomplished through Microsoft Purview Data Lifecycle Management (DLM).

**Set retention policies.** Retention policies are the cornerstone of data lifecycle management, and they can be used for Microsoft 365 workloads including Exchange, SharePoint, OneDrive, Teams, and Yammer. You can configure whether content for these services needs to be retained indefinitely, for a specific period after users edit or delete it, or if it should be automatically permanently deleted after a specified period. For instance, you could set academic records for a certain school year to expire at a particular interval after the school year ends, depending on what your local and institutional regulations dictate.

When you configure a retention policy, you can target all instances in your institution (such as all mailboxes and all SharePoint sites), or individual instances (such as only the mailboxes for specific departments, or just selected SharePoint sites or Class Teams). If you need exceptions for individual emails or documents, such as a longer retention period for legal documents, you do this with retention labels. These can be published to apps so that students and faculty can apply them, or automatically applied to content that matches specific conditions.

## Classify and protect sensitive items

**Retain sensitive information.** While DLM is best for establishing retention for workloads and mailboxes—as well as a baseline level of retention for files—Microsoft Purview Records Management is designed to retain specific items that are subject to legal requirements, such as transcripts or PII.

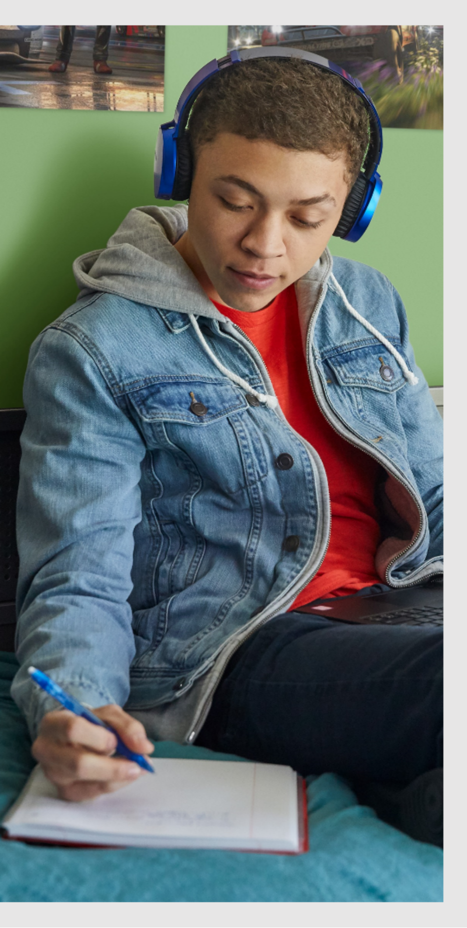
Especially with data volumes increasing and cybersecurity attacks on the rise, classifying and protecting this data is more important than ever.

**Label and encrypt sensitive items.** With Records Management, you can label and encrypt items so that only authorized users can access them. These labels apply even as data travels across systems. Microsoft enables you to classify items according to different levels of protection, from tagging data as *non-business* or *public* to *highly confidential*. In general, it's good practice to mark PII, health records, legal documents, academic records (such as disciplinary records, grades, and test scores), information security documentation, and confidential executive documents (such as board meeting notes or strategic plan drafts) as *highly confidential*.

Once a label is applied to a file, you can define and set policies that protect it when a potentially un-secure action is taken. For example, if a user tries to send an email that contains credit card numbers or a document labeled as *highly confidential*, the system can block recipients from receiving it or accessing its contents. Even when data leaves your organization's boundaries, its protection settings remain in place to ensure only permitted users have access to confidential or sensitive data.

## Manage legal holds

**Locate and export information.** Finally, you need a way to locate and export content subject to legal hold requirements, such as transcripts, records, emails, and more. Once located, you not only need to hold data for the required times, but you also need to deliver it to the relevant parties as securely as possible. The consequences for failure can be substantial; not having proper tagging and retention procedures can result in reputational and financial impacts, making it essential that administrators have tools that provide visibility into the volume and location of sensitive data stored within their institution's systems.



With Microsoft Purview eDiscovery, you can locate and export content subject to hold requirements in Microsoft 365 and Office 365, and you can place an eDiscovery hold on content locations such as Exchange mailboxes, OneDrive accounts, SharePoint sites, and Microsoft Teams. When you place a hold, you can assign permissions to IT, legal, and other teams so that they can access and manage cases.

**More easily fulfill subject rights requests.** At times, alumni, current students, or others associated with your institution may exercise their data protection rights and request access to data your institution holds about them. This may arise for reasons related to legal proceedings, applications to a new academic program, concerns about inaccurate information, and more.

With Microsoft Priva, you can more easily fulfill subject rights requests. Priva Subject Rights Requests supports four types of requests: access, export, tagged list for follow-up, and delete (preview). As soon as you create a request, Priva will identify the files, emails, sites, and chats that contain the subject's personal data, and the content will then be delivered to you within a few hours. If there's a large amount of data, Priva can suggest which items you should prioritize for review, and it will then generate a report to send to the data subject, audit logs, and a summary of tagged files so you can complete any follow-up actions.

# Unifying your data

It can be challenging to unify information that's stored across systems due to varying data formats, storage systems, and database structures, but a united data estate presents ample opportunities for education, including improved decision-making and resource allocation. Using the Dynamics 365 education accelerator, administrators can eliminate data silos and integrate data from multiple sources, leveraging the education data model and sample applications to make the most of their data. The education data model provides custom tables for higher education and K-12 use cases, which can be extended to build applications on Power Platform and Dynamics 365. This opens up a world of possibilities for institutions to visualize data in new ways, surface it in new contexts, and build solutions tailored for the needs of their constituents.

# Additional resources and guidance

## Microsoft partners

Explore the information and storage solutions provided by our global network of partners. For regional availabilities and solution details, visit our partners' websites.

| Solution area | Partner name | | |
|---|---|---|---|
| Gain visibility, set policies, and manage lifecycles | AvePoint<br>Cognillo<br>CoreView | Infotechtion<br>Manage Engine<br>ProvisionPoint | Quest<br>ShareGate<br>Syskit |
| Clean up inactive files and accounts | AvePoint<br>Cognillo<br>Infotechtion | Manage Engine<br>Quest | ShareGate<br>Syskit |
| Allocate storage based on need | Globus<br>ProvisionPoint | Silk<br>Weka | |
| Adapt to compliance and grant requirements | AvePoint<br>CoreView<br>Epiq Global | Exelegent<br>Infotechtion<br>Manage Engine | Netwoven<br>Perficient<br>Protiviti |
| Enable secure external file sharing | Cyclotron<br>Globus<br>Netwoven | Quest<br>ShareGate | |
| Classify and protect sensitive items | AvePoint<br>Infotechtion<br>Protiviti | Quest<br>ShareGate | |
| Manage workload retention and legal holds | AvePoint<br>Epiq Global | Infotechtion<br>Protiviti | |

# Learn more

Learn more about how you can simplify information lifecycle and storage management at your institution using the following resources.

## Microsoft 365 resources

- Microsoft 365 Storage Guidance: Learn about the resources available to you when managing storage for certain applications in Microsoft 365.
- Microsoft 365 End User Guidance: Understand how to convey Microsoft's storage limits to your students and end users and promote good storage habits in OneDrive and Outlook.
- How OneDrive safeguards your data in the cloud: Learn about OneDrive's data protection practices and how you can protect your data in OneDrive.
- SC-400: Implement Data Lifecycle and Records Management: Get experience planning and implementing data lifecycle and records management strategies with this training on Microsoft Learn.

## Azure resources

- Microsoft Azure: Learn more about Azure's capabilities, use cases, and features.

## General resources

- Microsoft Purview compliance documentation: Learn more about Microsoft Purview compliance on Microsoft Learn.
- Deploy an information protection solution with Microsoft Purview: Discover how you can use Microsoft Purview to develop a comprehensive information protection framework.
- Microsoft Purview Data Lifecycle Management: Learn to use Microsoft Purview Data Lifecycle Management to reduce your storage space.
- Microsoft Purview Compliance Manager: Discover Microsoft Purview Compliance Manager features and use cases.
- Learn about retention policies & labels to retain or delete: Get guidance on using retention policies and labels.
- Microsoft Purview eDiscovery solutions: Learn about Microsoft's suite of eDiscovery solutions.

Microsoft