

---

# Managing records in Microsoft 365

---

Guidance for NSW public offices

**Version 1.0**

**5 May 2025**

This guide has been developed for State Records NSW by Andrew Warland, a consultant with many years of experience advising organisations on how to implement Microsoft 365 for effective recordkeeping. This guidance may be used and adapted by organisations for their own purposes.

*The content is accurate as of 5 May 2025 but will lose currency over time, as Microsoft makes changes to system functionality.*

**State Records Authority NSW**

## Copyright Statement

©



Except for any logos, emblems, and trademarks, this work is licensed under a Creative Commons Attribution 4.0 International license, to the extent that it is protected by copyright. Authorship of this work must be attributed to State Records NSW. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/legalcode>

## Disclaimer

The State of New South Wales gives no warranty that the information in this version is correct or complete, error free or contains no omissions. The State of New South Wales shall not be liable for any loss caused due to negligence or otherwise arising from the use of this Guide.

# Contents

<b>Introduction and purpose</b>	<b>5</b>
<b>Part 1 – Overview to managing records in Microsoft 365</b>	<b>6</b>
What is Microsoft 365?	6
Accessing Microsoft 365	6
Licensing Agreements	7
Tenant	7
Accounts	7
Admin Roles	8
Admin roles in public offices that are part of a multi-tenant or outsourced IT arrangement	8
Privileged and non-privileged roles	8
Privileged Identity Management and Privileged Access Management	9
Other roles in Exchange Online admin and Purview centres	10
What roles are needed to manage records?	10
SharePoint Site Collection Administrator role	12
Licences	12
Microsoft 365 is an ‘evergreen’ service	13
<b>Part 2 – Administration of and governance for Microsoft 365</b>	<b>14</b>
Governance for Microsoft 365	17
Monitoring Microsoft 365	18
Microsoft 365 admin centre	18
SharePoint admin centre	19
Microsoft Purview	19
<b>Part 3 – Where are the records created, captured and stored in Microsoft 365?</b>	<b>20</b>
Records in Microsoft 365 are stored in ‘workloads’	20
The relationship between Microsoft 365 Groups and Teams	23
The Azure substrate	24
<b>Part 4 – Configuring Microsoft 365 and SharePoint Online to manage records</b>	<b>25</b>
Exchange Online admin	25
Microsoft Entra	26
Microsoft 365 admin centre	27
Teams admin	28
SharePoint/OneDrive admin	29
<b>Part 5 – Architecture approach for managing records in SharePoint</b>	<b>34</b>
OneDrive is a SharePoint service	35
Guiding principles	35
SharePoint site types	35
Value and risk	36
Requests for new SharePoint sites and Teams	38
Provisioning new SharePoint sites	41
Configuring individual SharePoint sites to manage records	44
Site columns (metadata) and content types	44
Create activity-based libraries to aggregate related records	45
Configuring document libraries	46

Site contents	50
Disposal process/stubs	51
What happens to records and other content that is destroyed?	52
<b>Part 6 – Compliance in Microsoft Purview</b>	<b>53</b>
Audit logs	53
eDiscovery and Content Search	54
Retention for content in Microsoft 365 – policies or labels?	57
Data Lifecycle Management	59
Retention policies	60
Retention labels	62
Alternatives to retention policies or labels	70
Adaptive scopes	71
Legacy Exchange Online Messaging Records Management	72
Information sensitivity labels	74
Data Loss Prevention	79
Communication Compliance	79
Insider Risk Management	79
Compliance Manager	80
AI and Machine Learning classifiers, Data explorers (E5)	81
Classifiers	82
Explorers	82
<b>Attachment A – Recommended retention policies</b>	<b>85</b>
Retention policy for personal and shared mailboxes	85
Retention policy/ies for OneDrive	86
Retention policy/ies for Microsoft 365 Groups (Exchange mailbox and SharePoint site)	87
Retention policy/ies for non-Group-based SharePoint sites	88
Retention policy/ies for Teams chats	89
Retention policy/ies for Microsoft Copilot experiences	90
Retention policy/ies for Enterprise AI apps	91
Retention policy/ies for Teams (standard and shared) channel posts	92
Retention policy/ies for Teams private channel posts	93
<b>Attachment B – Pay-as-you-go subscription services</b>	<b>94</b>
SharePoint Advanced Management	94
Microsoft Syntex	94
AI Builder	95
Copilot	95
<b>Attachment C – Microsoft 365 admin centres</b>	<b>97</b>
<b>Additional resources</b>	<b>102</b>

# Introduction and purpose

The *State Records Act 1998* requires each public office to ‘make and keep full and accurate records of the activities of the office’, to ‘establish and maintain a records management program for the public office’ (section 12) and to maintain accessibility to equipment/technology dependent records (section 14). Section 21 of the Act prohibits the abandonment, disposal, transfer, damage or neglect of State records.<sup>1</sup>

The purpose of this document is to provide guidance to NSW government public offices on the management of records created or captured across Microsoft 365, supporting and consistent with guidance provided in relevant NSW government standards and guidelines, including guidance on Microsoft 365 and recordkeeping.<sup>2</sup>

The document includes:

- General information about Microsoft 365.
- Suggestions and (where appropriate) recommendations for the configuration of settings relating to the management of records across Microsoft 365.
- Details of an approach to information architecture in SharePoint Online.

## Disclaimer

The content in this document was accurate as of 5 May 2025. As Microsoft 365 is an ‘evergreen’ service, some of the details provided in this document may change.

---

<sup>1</sup> **Source:** [Introduction to the Standard on records management | NSW Government](#) (accessed 5 May 2025)

<sup>2</sup> **See:** [Microsoft 365 and recordkeeping | NSW Government](#) (accessed 5 May 2025)

# Part 1 – Overview to managing records in Microsoft 365

## What is Microsoft 365?

Microsoft 365 is a subscription-based service that provides organisations with access to a range of productivity applications, cloud services and storage<sup>3</sup>, and security and compliance features.

The actual applications, services and features that can be accessed depends on the types of licences that are acquired (see below) and whether an organisation has its own Microsoft 365 tenant or is part of a multi-tenant arrangement. See below for the definition of 'tenant'.

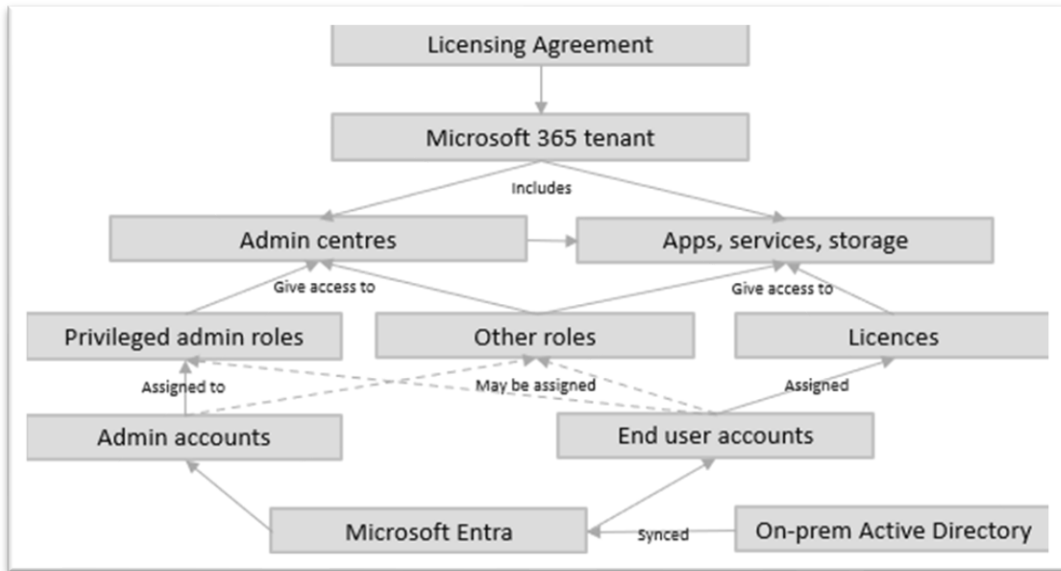
## Accessing Microsoft 365

As shown in the diagram below, access to Microsoft 365 requires:

- One or more licensing agreements with Microsoft, for example an Enterprise Agreement, Cloud Agreement, or Products and Services Agreement.
- The existence of a tenant that provides access to various admin centres, applications, services and storage (subject to licencing).
- The existence and/or creation of admin and accounts in Microsoft Entra, usually synced from an on-premises Active Directory. See below for the definition of 'account'.
- The purchase and assignment of licences to accounts.
- The assignment of admin roles to admin accounts, and the (optional) assignment of some roles to some accounts (for example, an end-user account assigned to the Global Reader role).

---

<sup>3</sup> The 'cloud' refers to an 'online storage space where people and businesses store their files and applications, accessible from anywhere with an internet connection'. The cloud also offers 'services, such as computing power, databases, networking and software applications'. Source: What is the cloud? | Microsoft Azure (*accessed 2 May 2025*)



**Image:** Access to Microsoft 365 requires the existence of a licensing agreement which provides access to a tenant, and user accounts that are assigned licences and roles. Notes: (1) Entra was previously known as Azure Active Directory. (2) Admin accounts are not normally assigned licences. (3) Some end user accounts may be assigned a role, including a privileged role.

## Licensing Agreements

Licensing agreements determine what Microsoft 365 (and other Microsoft) services organisations can access.<sup>4</sup>

## Tenant

Microsoft defines a Microsoft 365 tenant as ‘a dedicated instance of the services of Microsoft 365 and your organisation data stored within a specific default location, such as Europe or North America. This location is specified when you create the tenant for your organisation. Each Microsoft 365 tenant is distinct, unique, and separate from all other Microsoft 365 tenants.’<sup>5</sup>

NSW government public offices may either have their own tenant or be part of a multi-tenant arrangement. Public offices in multi-tenant arrangements do not have access to the various administrative elements of Microsoft 365 which can limit their ability to access and implement various recordkeeping functionality.

## Accounts

When a tenant is created, at least two Global Administrator (‘Global Admin’) roles are created, including one ‘break-glass’ account that is only used if other Global Admins are locked out. These roles should be assigned to ‘as few as possible’ cloud-only dedicated admin accounts.<sup>6</sup>

<sup>4</sup> Source: [Microsoft Licensing Agreements](#) (accessed 2 May 2025)

<sup>5</sup> Source: [Tenant management for Microsoft 365 for enterprise | Microsoft Learn](#) (accessed 2 May 2025)

<sup>6</sup> Source: [About admin roles in the Microsoft 365 admin center - Microsoft 365 admin | Microsoft Learn](#) (accessed 2 May 2025)

The tenant's Global Admins will then arrange for other accounts to be created in Microsoft Entra (the cloud-based directory services). This is typically achieved by syncing existing accounts from an on-premises<sup>7</sup> Active Directory.<sup>8</sup>

Note: When a new account is created, the account holder may be able to access the Microsoft 365 portal ('office.com') but will have no access to any applications or services until they are assigned a licence or a role.

## Admin Roles

Every Microsoft 365 tenant will have a small number of Global Admins which is one of several 'privileged' roles (see below). Microsoft recommend limiting the number of Global Admins to no more than three dedicated admin accounts as these admins have 'almost unlimited access to an organisation's settings and most of its data'.<sup>9</sup>

- Public offices in multi-tenant environments or with outsourced IT arrangements need to understand and consider the potential risks associated with their IT provider having this level of access. At a minimum, they should know who has been assigned the Global Admin role and be able to request reports on that role's activities in relation to their content. For example, an audit report that shows what files were accessed, downloaded or deleted.

Global Admins are responsible for setting up various other admin roles, for example the Exchange Online Administrator or the SharePoint Administrator, as well as numerous other 'minor' roles such as User Administrator or Billing Administrator.

## Admin roles in public offices that are part of a multi-tenant or outsourced IT arrangement

End user accounts in public offices that are part of a multi-tenant environment will rarely if ever be assigned any admin role because these roles provide access to configuration settings and content stored across the tenant.

Public offices with their own tenant that have outsourced their IT services might consider requesting access to at least one admin account assigned the Global Admin (or even the read-only version, Global Reader) role. They should be able to request the configuration changes as described in this document.

## Privileged and non-privileged roles

There are two types of admin role in Microsoft 365: privileged and non-privileged.

There are more than 25 privileged roles, including the Global Admin role, in Microsoft 365. According to Microsoft, privileged roles should always be assigned to dedicated admin accounts as '(they) can be used to delegate management of directory resources to

---

<sup>7</sup> 'On-premises software (abbreviated to on-prem, and often written as 'on-premise') is installed and runs on computers on the premises of the person or organisation using the software, rather than at a remote facility such as a server farm or 'cloud.'  
**Source:** [On-premises software - Wikipedia](#) (accessed 2 May 2025)

<sup>8</sup> **Source:** [Active Directory Domain Services Overview | Microsoft Learn](#) (accessed 2 May 2025)

<sup>9</sup> **Source:** [About admin roles in the Microsoft 365 admin center - Microsoft 365 admin | Microsoft Learn](#) (accessed 2 May 2025)

other users, modify credentials, authentication or authorization policies, or access restricted data.<sup>10</sup>

Privileged admin roles should give only the access required to get the job done, with strong additional security controls (see below) to minimise the risk of compromise. Organisations may use a role-based access control ('RBAC') model to help manage this outcome.<sup>11</sup>

In addition to the Global Admin role, the other privileged roles include the Security Administrator, Authentication Administrator, Cloud Device Administrator, Conditional Access Administrator, Global Reader, Intune Administrator, Password Administrator, User Administrator, and Application Administrator.<sup>12</sup>

Microsoft recommends that no more than 10 (dedicated admin) accounts should be assigned to these privileged roles.<sup>13</sup>

- Public offices in multi-tenant environments or with outsourced IT arrangements should request a listing of all accounts assigned to every admin role. Ideally, this detail should be included in an RBAC matrix.

There are at least 100 non-privileged roles. These roles allow organisations to be very specific about which account can access (via the role) what functionality. For example:

- The SharePoint Admin role gives the account holder access to the SharePoint admin centre (and parts of the Microsoft 365 admin centre).

The User Administrator role gives the account holder access to the area of the Microsoft 365 admin centre used to manage users (and some other areas).

## Privileged Identity Management and Privileged Access Management

Both privileged and non-privileged roles may be subject to time-limited and approval-based access via Privileged Identity Management (PIM) as shown in the Microsoft image below.

- For example, if a records or information manager needs to access Microsoft Purview to set up retention policies, the Compliance Administrator role could be made 'eligible' for PIM access on a time-limited basis. The records or information manager requests access to the role and, when granted access, will be able to access Purview with that role for the period of time set in the PIM rule.

An additional level of control known as Privileged Access Management (PAM) may also be applied to limit what tasks each role can do.

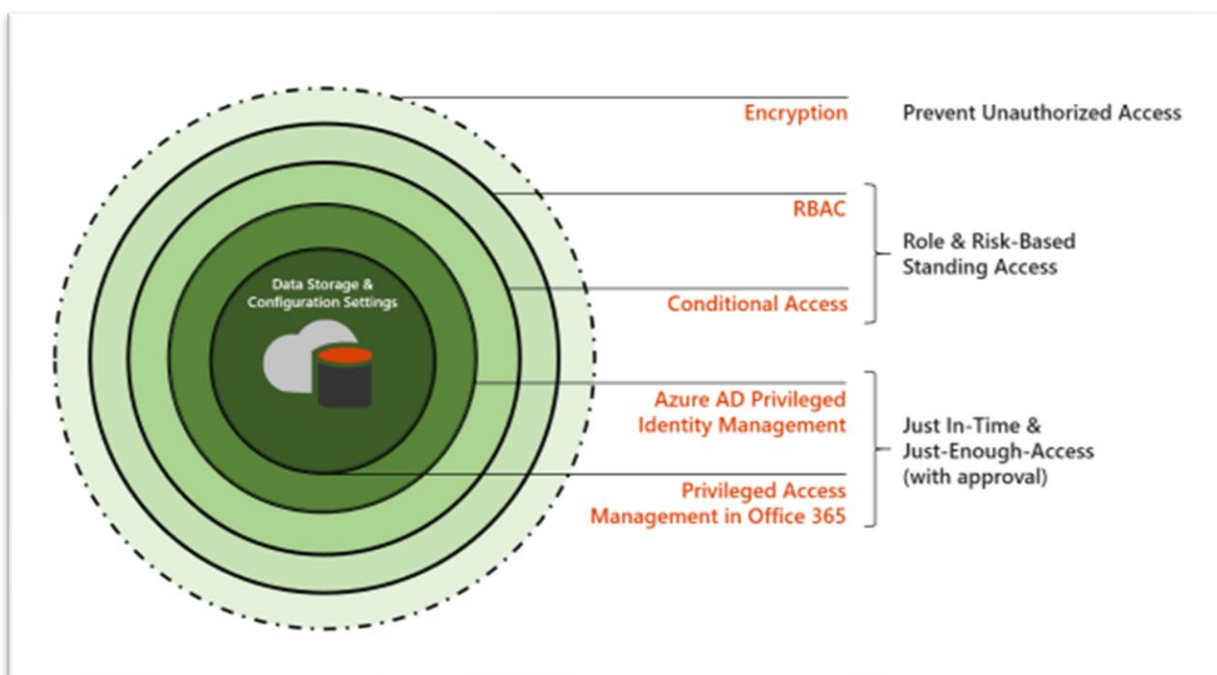
---

<sup>10</sup> **Source:** [Privileged roles and permissions in Microsoft Entra ID \(preview\) - Microsoft Entra ID | Microsoft Learn](#) (accessed 2 May 2025)

<sup>11</sup> **Source:** [Overview of Microsoft Entra role-based access control \(RBAC\) - Microsoft Entra ID | Microsoft Learn](#) (accessed 2 May 2025)

<sup>12</sup> For the full list, see [About admin roles in the Microsoft 365 admin center - Microsoft 365 admin | Microsoft Learn](#) (accessed 2 May 2025)

<sup>13</sup> **Source:** [About admin roles in the Microsoft 365 admin center - Microsoft 365 admin | Microsoft Learn, Best practices for Microsoft Entra roles - Microsoft Entra ID | Microsoft Learn](#) (accessed 2 May 2025)



*Image: Layers of protection for Microsoft 365 services<sup>14</sup>*

## Other roles in Exchange Online admin and Purview centres

In addition to the admin roles described above, there are another 29 ‘admin role groups’ in the Exchange Online admin centre, each with a specific set of permissions. For example, one of these permissions controls the ability to access the audit logs in Purview.<sup>15</sup>

Microsoft Purview includes a series of ‘role groups’ (some of which are the same as in Exchange admin) that are required to access certain areas of Purview or specific features. For example:

- The ‘Records Management’ role group provides the ability to configure and implement retention policies and labels.
- The Content Explorer List Viewer and Content Explorer Content Viewer role groups provide the ability to drill down to items in the Data Explorer (previously the now ‘classic’ Content Explorer) area of the Explorers view in various Purview sections (described in the Purview section below).<sup>16</sup>

Few of the role groups in Exchange Online or Purview are eligible for PIM.

## What roles are needed to manage records?

As noted already, public offices that are part of a multi-tenant environment, and records and information managers in those public offices, will rarely if ever be assigned any admin accounts or roles because they provide access to content across the entire tenant. This limits the ability of records and information managers to manage records. At

<sup>14</sup> **Source:** [Learn about privileged access management](#) | Microsoft Learn (accessed 2 May 2025)

<sup>15</sup> **Source:** [Permissions in Exchange Online](#) | Microsoft Learn (accessed 2 May 2025)

<sup>16</sup> **Source:** [Permissions in the Microsoft Purview portal](#) | Microsoft Learn (accessed 2 May 2025)

most, records and information managers may be assigned to the Site Collection Administrator role for the SharePoint sites (including sites linked with Teams) created for their organisation (see below). This role is the same one used by SharePoint admins to access SharePoint sites.

Individuals in public offices that have outsourced their IT, but are not in a multi-tenant environment, should consider requesting access to at least one dedicated admin account assigned to the Global Administrator role and also the Compliance Administrator role. These roles will give a public office access to all settings and monitoring functionality in Microsoft 365.

The recommended roles for records and information managers who are not part of multi-tenant environments are listed below.

Role	Rationale
<b>Global Reader*</b> Or <b>Reports Reader*</b>	This role can be used to monitor the environment, as it provides read only access to all Microsoft 365 admin centres including the usage reports in the Microsoft 365 admin centre.  This role provides access to the usage reports in the Microsoft 365 admin centre.
<b>Compliance Administrator*</b>  Or	This role is recommended for records and information managers (preferably with E5 licences) as it provides access to most of the features in Microsoft Purview, including audit logs, eDiscovery, retention policies and labels, information sensitivity labels and policies, data classification/content explorer (subject to licence type), compliance manager, data loss prevention, and multiple other features.
<b>eDiscovery Manager (Purview assigned role)</b>  Or  <b>Records Management (Purview assigned role group)</b>	This role is recommended for legal and anyone responsible for freedom of information type requests. It provides access to the eDiscovery (standard and premium) and global content search capabilities in Purview and some other functionality as well, but not the retention policy elements of Data Lifecycle Management or Records Management.  This role provides access to many Microsoft Purview features, for example the Data Lifecycle Management (E3 and E5) and Records Management (E5) sections that are used to create, configure and implement retention policies and labels.
<b>SharePoint Administrator*</b>	SharePoint admin centre, all SharePoint sites (including those linked with a Team).

\*PIM eligible

## SharePoint Site Collection Administrator role

In addition to the above roles, records and information managers in both multi-tenant and non-multi-tenant organisations should ideally be assigned to the Site Collection role in every site in their tenant (or set of sites for multi-tenant public offices) to allow them to access and manage records on all sites 'owned' by the public office, including sites connected with individual Teams in Microsoft Teams and also the SharePoint sites linked with private and shared channels in Teams.

- An effective way to achieve this outcome is by (a) creating a dedicated security group that includes both the SharePoint 'technical' administrator/s as well as the records managers and (b) adding that Group to the Site Collection Administration section of every SharePoint site.

## Licences

Licences determine the applications that end users can access in Microsoft 365. Most public offices will have or acquire a combination of 'enterprise' ('E') level licences as described below.<sup>17</sup>

Licence type	Typical user	Provides access to
E5	Information worker and administrators	<p>This licence type provides access to most of the services and applications in Microsoft 365. Unless configured otherwise, it creates an Exchange Online mailbox, a OneDrive account, and gives the account holder access to Office applications on their desktop and in the cloud.</p> <p>When coupled with specific roles (such as Compliance Administrator) this licence allows records and information managers to create retention policies, and access a range of advanced options in Microsoft Purview including: AI and Machine learning tools; the ability to auto-apply sensitivity labels in Exchange, SharePoint and OneDrive; use Machine Learning-based and rules-based automatic retention labels; and access the added functionality such as 'Disposition' in the 'Records Management' section of Purview.</p> <p>It allows end users to auto-apply sensitivity and retention labels and set default sensitivity labels for SharePoint document libraries.</p>
E3	Information worker and administrators	<p>This licence type provides most of the functionality required by information workers. Unless configured otherwise, it creates an Exchange Online mailbox, a OneDrive account, and gives the account holder access to Office applications on their desktop and in the cloud.</p> <p>For records and information managers, when coupled with a specific role (such as Compliance Administrator), it also</p>

<sup>17</sup> **Source for licencing information:** [Compare Microsoft 365 Enterprise Plans | Microsoft 365](#) (select the 'Get full comparison table' link to access the PDF file)

---

provides the ability to create retention policies and sensitivity and retention labels.

It allows end users to manually apply sensitivity labels and retention labels.

<b>F3</b>	Frontline workers	A limited set of options including Microsoft 365 for mobile and the web, a 2 GB Exchange Kiosk mailbox (but not Outlook), SharePoint Kiosk (online only) with 2 GB OneDrive storage, Microsoft Planner, Microsoft To-Do, Viva Engage (formerly Yammer), the ability to manually apply sensitivity labels and retention labels.
<b>F1</b>	Frontline workers	An even more limited set of options, including Microsoft Teams and Microsoft Planner, SharePoint Kiosk with 2 GB OneDrive storage. It includes the ability to manually apply sensitivity labels and retention labels.

---

In addition to the above, public offices may also acquire licences for:

- Other Microsoft applications such as Microsoft Project or Dynamics 365.
- Add-on services such as Copilot.
- Subscription-based services such as Microsoft Syntex. See Attachment A for the list of these services.

## Microsoft 365 is an ‘evergreen’ service

As with other online subscription services, Microsoft may add, modify, remove or deprecate various functionality or features in Microsoft 365 from time to time. This type of constant change is known as ‘evergreen’.

Despite its ‘evergreen’ nature, much of the core underlying architecture of Exchange Online and SharePoint Online where most records are stored has remained largely the same for many years.

Almost all forthcoming changes are described in the Microsoft 365 roadmap and announced in advance via the Message Centre in the Microsoft 365 admin centre.

- <https://www.microsoft.com/en-us/microsoft-365/roadmap> (public web site)
- <https://admin.microsoft.com/Adminportal/Home#/MessageCenter> (opens your tenant’s Microsoft 365 admin centre. The link will not be accessible if you don’t have the required role)

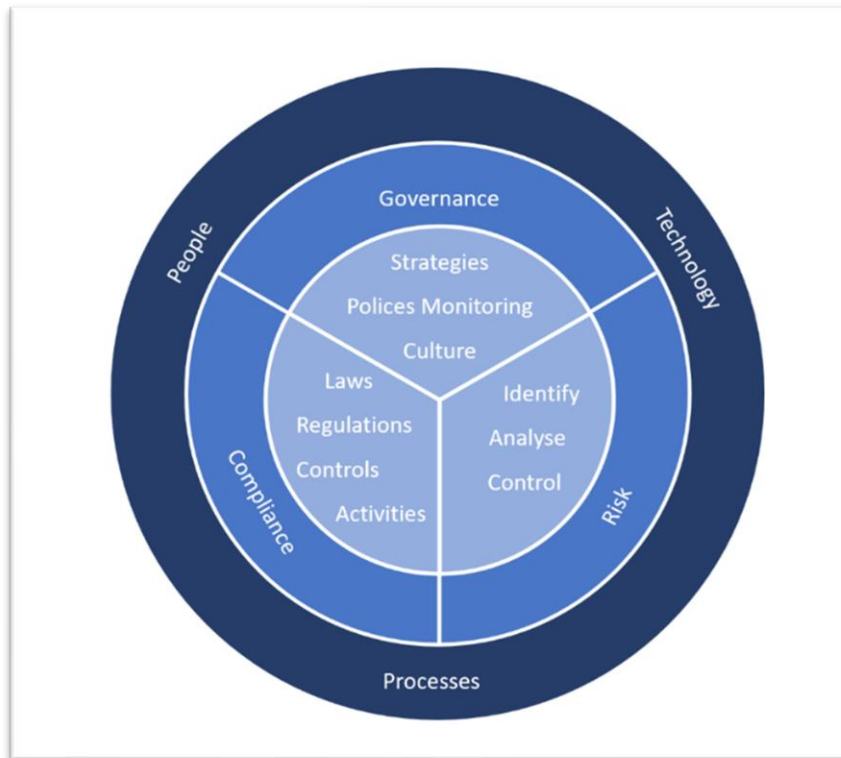
Public offices should:

- Review messages in the Message Centre at least monthly to determine what action may be required, including for change management purposes, and to determine the potential impact on integrations with other applications.
- Plan to retire and/or avoid implementing any feature that Microsoft have advised will be deprecated in the future or is described as ‘classic’.

Public offices that do not have access to the Microsoft 365 admin centre should seek regular updates from their IT provider.

## Part 2 – Administration of and governance for Microsoft 365

Governance is a key element for the effective use and management of Microsoft 365. The image below is from the Microsoft 365 Maturity Model.<sup>18</sup>

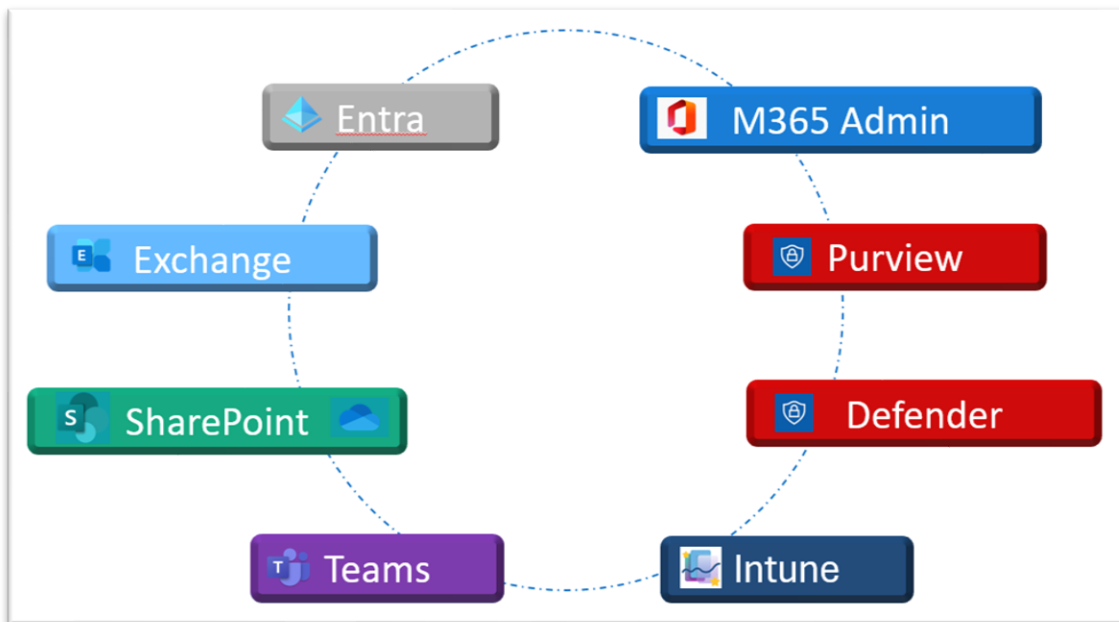


*Image: The Microsoft 365 Maturity Model*

Records and information managers should aim to develop a good understanding of, and play an active role in governance for, the Microsoft 365 environment.

Microsoft 365 has eight interconnected admin centres as shown in the diagram below. Global administrators are primarily responsible for Entra and Microsoft 365 admin centres but can access all other admin centres. Other admin roles provide access to the other admin centres, for example an Exchange administrator will be assigned to the Exchange admin role giving them access to the Exchange admin centre.

<sup>18</sup> See: [The Microsoft 365 Maturity Model – Governance, Risk, and Compliance Competency | Microsoft Learn](#) (accessed 2 May 2025)



*Image: Microsoft 365 admin centres*

Each of the above admin centres has a specific purpose:

- **Microsoft Entra** (formerly Azure Active Directory), used to manage identity and network access. According to Microsoft, Entra enables organisations ‘to implement a security strategy and create a trust fabric that verifies identities, validates access conditions, checks permissions, encrypts connection channels, and monitors for compromise’.<sup>19</sup> It includes a range of configuration options that can impact the management of records, such as:
  - The ability to create new, and auto-expire unused, Microsoft 365 Groups. Restricting the ability to create new Microsoft 365 Groups prevents end users from creating Teams and Group-based SharePoint sites.
  - The creation of conditional access policies that can be used to limit what end users can do, including, in combination with information sensitivity labels, to restrict what users can do with content classified with these labels, or from what IP address or domain.
  - The ability to invite or block external guest users and control what they can access.
  - The assignment of roles via Privileged Identity Management.
- **Microsoft 365 admin**, used to manage common administrative tasks (and Global Readers with the ability to view most of the settings).<sup>20</sup> It provides:
  - Access to the list of existing users and guests, and the ability to create new ones.
  - Access to the list of existing Microsoft 365 Groups and Teams, Security Groups, and Distribution Lists and the ability to create new ones.
  - The ability to access a user’s OneDrive account.
  - Access to centralised Search and Intelligence capabilities, to see what end users are searching for.

<sup>19</sup> **Source:** [What is Microsoft Entra? - Microsoft Entra | Microsoft Learn](#) (accessed 2 May 2025)

<sup>20</sup> **Source:** [Microsoft 365 admin center - Overview - Microsoft 365 admin | Microsoft Learn](#) (accessed 2 May 2025)

- Access to reports and dashboards that can be used to monitor where records may be stored in Outlook, Teams, SharePoint and OneDrive.
  - Access to the full range of configuration settings, including settings that can impact the management of records.
  - Access to the Message Centre.
  - Shortcuts to all other admin centres.
- **Exchange Online admin**, used to manage all aspects of Exchange and Exchange mailboxes. Note:
    - Management of the now-legacy ‘Messaging Records Management’ (MRM) policies and tags is now done in Purview.
    - Both personal and Group-based Exchange mailboxes contain significantly more content than their on-prem predecessors, much of it stored in hidden folders. This includes the hidden folder ‘Teams messages data’ that is used to store ‘compliance copies’ of Teams chats and channel messages. The existence of so many hidden folders may affect the restoration of mailboxes from a backup solution.
- **Teams admin**, used to manage all aspects of Teams. It includes several settings that can impact the management of records, including:
    - The ability to create private and shared channels, both of which create new SharePoint sites that can be difficult for records and information managers to access (or know about).
    - Auto expiration (e.g., auto-deletion) for Teams recordings that are usually stored in OneDrives. This capability should be understood in the context of retention policies that will *prevent* their deletion.
- **SharePoint Online admin**, used to manage all aspects of SharePoint and OneDrive. SharePoint admins may also manage SharePoint and OneDrive using PowerShell.
- **Intune**, used ‘to manage user access to organisational resources and simplify app and device management across devices, including mobile devices, desktop computers, and virtual endpoints.’<sup>21</sup>
- **Purview**, a ‘data governance and compliance’ admin centre that includes the following records-related functionality (among other functionality):
    - Access audit logs relating to all activity across Microsoft 365.
    - Create content searches and create eDiscovery cases to search for content across Exchange Online mailboxes, Teams chats and channel messages, SharePoint sites and OneDrive, and place that content (or review sets) on legal hold and then export it.
    - Gain visibility into information stored across the organisation using AI and Machine Learning tools.
    - Create and implement information sensitivity labels and data loss prevention (DLP) policies.
    - Create and implement retention policies and labels. This is a key area and functionality of Purview that records managers need to understand well.
    - Create and implement Insider Risk Management policies.<sup>22</sup>

<sup>21</sup> **Source:** [What is Microsoft Intune | Microsoft Learn](#) (accessed 2 May 2025)

<sup>22</sup> **Source:** [Learn about Microsoft Purview | Microsoft Learn](#) (accessed 2 May 2025)

- **Defender**, described as a ‘threat protection and remediation suite of products and solutions that enables businesses to maintain the highest-level security posture across their cloud, Office 365, endpoint, application, and identity solutions’. Defender can be used to create and implement event policies to send notification when certain events occur, for example when a user downloads or deletes a certain number of items within a given period.<sup>23</sup>

Settings that relate (or could relate) to the management of records across these admin centres are included in Part 4 of this document.

## Governance for Microsoft 365

Microsoft recommends that organisations take a structured approach to managing governance, risk and compliance for Microsoft 365.<sup>24</sup>

Public offices should establish a governance committee and framework for Microsoft 365. The committee should include key representatives from IT (including the Microsoft 365 service owner and at least one Global Admin) as well as key records and information managers.

- Where a public office is part of a multi-tenant environment, it should seek details about its part of the tenant and is kept informed of all changes in the environment by the provider.
- Where a public office has outsourced its IT, it should work with the outsourced provider to establish roles and responsibilities and participate in regular meetings or other methods to be kept informed of all changes in the environment, including configuration changes.

Governance committees should be responsible for the following:

- Reviewing forthcoming changes to the environment to determine what change management or other actions may be required.
- Reviewing and approving proposed configuration changes, except where these are entirely ‘business as usual’. For example, there is no requirement for the committee to review the creation of every new SharePoint site or Team. However, there is a requirement for the committee to agree on retention rules and disposal actions for content that may be stored in the various Microsoft 365 workloads.
- Discussing issues and options that could affect the entire environment. For example, a decision to implement AI tools.
- Monitoring activity and volumes. This may include reviewing the output of AI and Machine Learning-based classification tools.
- Reviewing security incidents (unless these are subject to a separate security committee).

Establishing governance for Microsoft 365 will assist public offices to comply with Principle 1 of the Standard on records management<sup>25</sup> that states that organisations

<sup>23</sup> **Source:** [Training for Defender | Microsoft Learn](#) (accessed 2 May 2025)

<sup>24</sup> **Source:** [The Microsoft 365 Maturity Model – Governance, Risk, and Compliance Competency | Microsoft Learn](#) (accessed 2 May 2025)

<sup>25</sup> **See:** [Standard on records management | NSW Government](#) (accessed 5 May 2025)

should take responsibility for records and information management by establishing governance frameworks for the management of records, information and data.

## Monitoring Microsoft 365

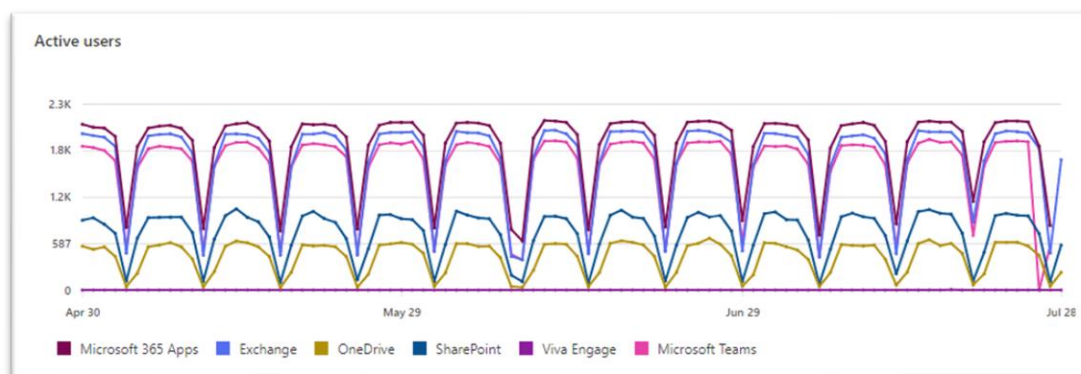
The Standard on records management requires organisations to take responsibility for records and information management, and to manage records and information and data well. Requirement 1.8 states that records and information management should be monitored and reviewed to ensure that it is performed, accountable and meets business needs.

In support of the Standard, records managers should regularly monitor both content and activities across Microsoft 365, to understand both where the records are (and also where they should not be stored) and how they are being used. Microsoft 365 includes functionality to support this monitoring.

Records and information managers who have been assigned the Global Reader role (including via Privileged Identity Management) can access a range of dashboards and other reports to monitor and manage records stored across the four primary workloads<sup>26</sup> in Microsoft 365 environment (Exchange Online, Microsoft Teams, SharePoint Online, OneDrive), as described below.

### Microsoft 365 admin centre

- Teams & Groups, to cross reference the list of SharePoint sites (see below) and to help with identifying if any SharePoint sites are 'missing' Groups or where Groups are ownerless (i.e., the former owner/s no longer work in the organisation).
- Settings – Search & Intelligence, to see what users are searching for and develop questions and answers to help them find it.
- Reports – Usage, to review all activity including volumes of content stored in both SharePoint and OneDrive.
- Health – Message Centre, to review change updates.



*Image: Example of a report showing active users for the various applications over a 90-day period in the Microsoft 365 admin centre*

The image below shows the OneDrive section of the usage reports area of the Microsoft 365 admin centre (third point above), showing the Owner, Last activity date, Files, Active Files and Storage used for each active OneDrive. Records managers should be given access to this section via the Global Reader role, to enable them to monitor the size of

<sup>26</sup> A workload is defined by Microsoft as a collection of IT assets (servers, Virtual Machines, applications, data, or appliances) that collectively support a defined process. Exchange and SharePoint are primary workloads in Microsoft 365. **Source:** [Define and prioritize workloads for cloud adoption - Cloud Adoption Framework | Microsoft Learn](#) (Accessed 2 May 2025)

OneDrive accounts and allow them to be more proactive about these accounts before the account is deactivated. Alternatively, IT can export the listing for review.

URL	Owner principal name	Last activity date (UTC)	Files	Active files	Storage used (MB)
	ExampleUser@microsoft.com	Thursday, July 11, 2024	44	0	17
	peterparken@microsoft.com	Wednesday, May 29, 2024	14	0	5
	@t.com		2	0	0
	@microsoft.com		0	0	2
	@oft.com		0	0	2
	@sonmicrosoft.com		0	0	2

*Image: The OneDrive area of the usage reports in the Microsoft 365 admin centre.*

## SharePoint admin centre

- Sites – Active/Deleted sites, to view details of all active and deleted sites.
- Content services – Term store, to view or edit any taxonomies, and access the Content Type gallery.
- Reports – Data access governance, to review details of external sharing.

## Microsoft Purview

- Compliance manager, especially if the assessment against ISO 16175 is used, noting that this and other assessments in this section may include recommendations for improvement that public offices have investigated but may decide not to implement. This functionality is described in more detail in Part 6 of this document.
- Data classification, to see and access locations where content may be stored, based on built-in trainable classifiers and sensitive information types. This functionality is described in more detail in Part 6 of this document.

## Part 3 – Where are the records created, captured and stored in Microsoft 365?

A record is defined as:

- Any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means (State Records Act, s.3(1) Definitions).
- Information created or received and maintained as evidence and as an asset by an organisation, in pursuit of legal obligations or in the course of conducting business. (AS/NZS ISO 30300: 2020 – section 3.2.10)

A State record is defined as:

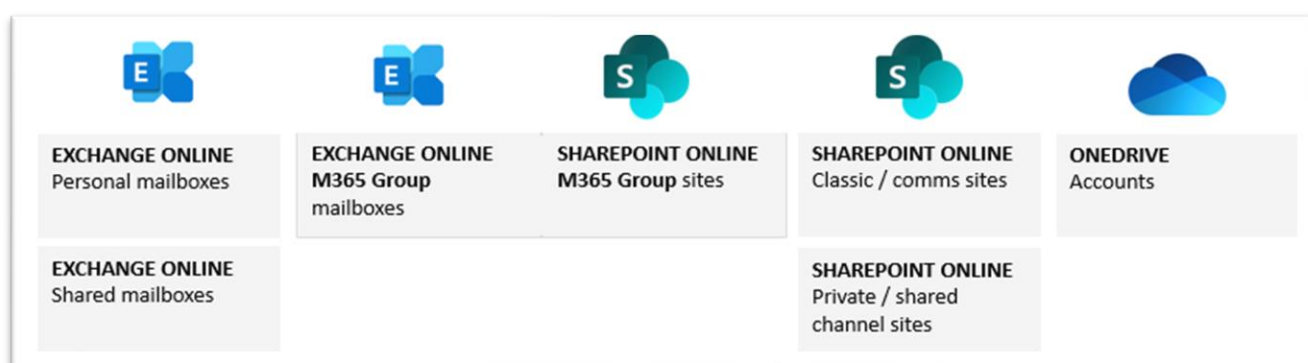
- a record made or received by a person, in the course of exercising official functions in a public office, or for a purpose of a public office, or for the use of a public office (State Records Act, s.3(1) Definitions).

Records provide evidence of business activities. Given the extent to which content is created, captured or stored by various Microsoft applications, such as Outlook, Teams, SharePoint and OneDrive, this means that almost anything created by a public office within the Microsoft 365 environment could be regarded as a record (and a State record) and must therefore be managed in accordance with the relevant records retention and disposal authority<sup>27</sup> and the Standard on records management.<sup>28</sup>

Although the definition of a record is all-encompassing, the rigour with which records are managed in Microsoft 365 may depend on an assessment of their value and the risks associated with them.

### Records in Microsoft 365 are stored in ‘workloads’

Most records will be captured or stored in one or more of the following ‘workloads’ in Microsoft 365. Note that ‘compliance copies’ of Teams chats and channels posts are stored in a hidden (and directly inaccessible) folder of either personal or M365 Group-linked Exchange Online mailboxes.



*Image: Microsoft 365 workload locations where records are likely to be stored*

<sup>27</sup> See: <https://www.nsw.gov.au/nsw-government/recordkeeping/records-retention-and-disposal-authorities>

<sup>28</sup> See: [Introduction to the Standard on records management | NSW Government](#), including requirement 2.4. (accessed 5 May 2025)

It is important to understand the concept of 'in-place', where records relating to the same subject may remain stored 'in-place' in different workloads. For example, an email may remain stored in an Exchange mailbox while content relating to the same subject may remain stored in a SharePoint document library.

The table below provides more detail about the content that is stored in each workload.

Workload	Visible	Hidden
Exchange Online personal mailboxes	<ul style="list-style-type: none"> <li>• Emails</li> <li>• Calendars</li> <li>• Notes</li> <li>• Tasks</li> </ul>	<ul style="list-style-type: none"> <li>• Compliance copies<sup>29</sup> of Teams 1:1 chats</li> <li>• Compliance copies of Teams private channel chats</li> <li>• Compliance copies of Viva Engage personal messages</li> <li>• Compliance copies of Copilot experiences</li> <li>• Compliance copies of other Enterprise AI apps</li> <li>• Other content, including Planner tasks</li> <li>• Soft-deleted emails that remain subject to a retention policy or label. These are stored in the Purges folder</li> </ul>
Exchange Online shared mailboxes	<ul style="list-style-type: none"> <li>• Emails</li> </ul>	
Exchange Online Microsoft 365 Group mailboxes	<ul style="list-style-type: none"> <li>• Emails</li> <li>• Calendars</li> </ul>	<ul style="list-style-type: none"> <li>• Compliance copies of Teams standard channel posts<sup>30</sup></li> <li>• Compliance copies of Viva Engage 'Community' messages</li> <li>• Soft-deleted emails that remain subject to a retention policy or label; these are stored in the Purges folder</li> </ul>

<sup>29</sup> A 'compliance copy' of Teams 1:1/many chats, or channel posts, is a copy of the original that remains stored in the (directly inaccessible) Azure Cosmos database. These copies are 'journalled' in (e.g., sent to) the 'TeamsMessagesData' hidden folder in the relevant personal or Group Exchange Online mailbox. This and other hidden folders cannot be directly accessed or modified but the content in some of them can be accessed from Purview using eDiscovery.

<sup>30</sup> A standard channel is one that is visible to all members of a Team. **Source:** [Standard channels in Microsoft Teams - Microsoft Teams | Microsoft Learn](#) (accessed 2 May 2025)

**Microsoft 365 Group-linked SharePoint Online sites (includes sites linked with a Microsoft Team)**

- Any type of digital item stored in document libraries, including via the 'Files' tab in a Teams channel. Includes the Group's OneNote, its WhiteBoard, Loop components<sup>31</sup>, and Teams recordings
- Items stored in lists
- Any content subject to a retention policy or label that has been deleted; these are stored in the site's Preservation Hold library that can be accessed by admins

**SharePoint Online sites linked with Teams private and shared channels**

- Any type of digital item stored in document libraries, including via the 'Files' tab in a Teams channel
- Any content subject to a retention policy or label that has been deleted; these are stored in the site's Preservation Hold library that can be accessed by admins

**SharePoint Online non-Group linked sites including communication and legacy sites**

- Any type of digital item stored in document libraries
- Items stored in lists
- Any content subject to a retention policy or label that has been deleted; these are stored in the site's Preservation Hold library that can be accessed by admins

**OneDrive**

- Any type of digital item stored in the document library, including via the 'Shared' (previously 'Files') tab in Teams chats. Includes a personal OneNote, Whiteboard, may also include Teams recordings
- Any content subject to a retention policy or label that has been deleted; these are stored in the OneDrive's Preservation Hold library that can be accessed admins

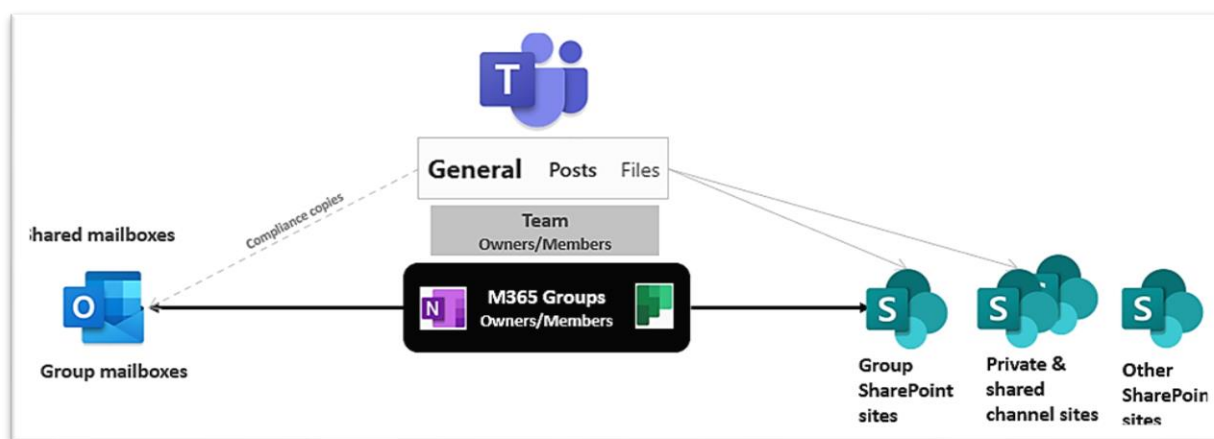
**Note:** There is currently no way to capture, download or save Teams chats or channel posts from the Teams interface. The only way to achieve this 'out of the box' is by taking a screenshot of the messages and saving the screenshot in a location where other records are stored. Teams chats and channel posts may however be searched for and accessed via a Content Search or an eDiscovery case in Purview.

<sup>31</sup> According to Microsoft, 'a Loop component is a portable piece of content that stays in sync across all the places that it is shared'. **Source:** [Get to know Loop components - Microsoft Support](#) (accessed 2 May 2025)

# The relationship between Microsoft 365 Groups and Teams

Microsoft 365 Groups are a core element in Microsoft 365. A good understanding of Microsoft 365 Groups is essential to understanding how to manage records in Microsoft 365.

According to Microsoft: 'Microsoft 365 Groups is the cross-application membership service in Microsoft 365. At a basic level, a Microsoft 365 group is an object in Microsoft Entra ID with a list of members and a coupling to related workloads including a SharePoint team site, shared Exchange mailbox, Planner, and OneNote notebook. You can add or remove people to the group just as you would any other group-based security object in Active Directory.'<sup>32</sup>



*Image: The relationship between a Microsoft 365 Group, its mailbox and SharePoint site, and a Team, as well as non-Group/Team sites*

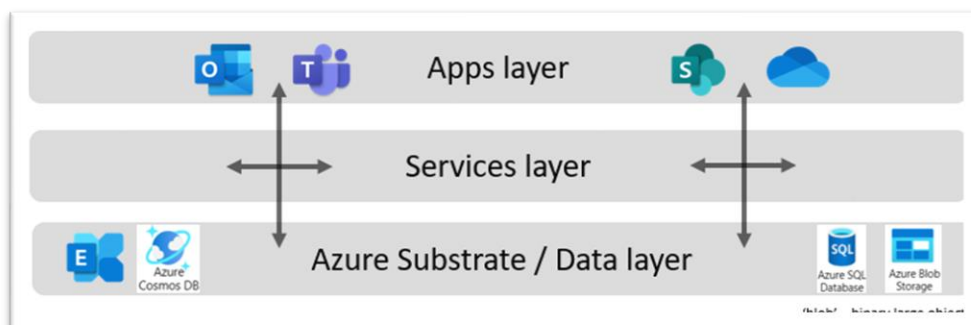
As shown in the diagram above, every Team in Microsoft Teams is directly linked with a Microsoft 365 Group.

- The Team owners and members are the same as the Microsoft 365 Group owners and members.
- External guests added to a Team are added to the Microsoft 365 Group (and vice versa).
- Content saved via the Files (to be renamed 'Shared' by mid-2025) tab in a Team's channel is saved directly to the Group's SharePoint site. There is no dedicated Teams 'files' storage; all the 'Files' content in a standard Teams channel is stored in the SharePoint site linked to the Group/Team.
- Private and shared channels create a new non-Group SharePoint site linked with the parent Group's SharePoint site (the private or shared channel site name follows the naming convention of 'Groupsitename-privatesharedchannelname').
- Tasks in Planner are stored in a separate Planner service, but tasks assigned to an end-user are stored in a hidden folder in personal mailboxes.
- A 'group' chat in the Team's chat area does not create a new Microsoft 365 Group.

<sup>32</sup> Source: [Microsoft 365 Groups and Microsoft Teams - Microsoft Teams | Microsoft Learn](#) (accessed 2 May 2025)

## The Azure substrate

All content created across Microsoft 365 is stored in the tenant-linked Azure storage area, known as the 'substrate'.



*Image: A simple visual representation of the relationship between the various layers in Microsoft 365*

The following points provide summary details about each workload where records are likely to be stored.

- The **Exchange Online** service is used to store emails as well as a range of other content. Each mailbox may contain over 500 folders, most of which are hidden.
- All Teams chats and posts are stored in a special instance of an **Azure Cosmos database**. This database cannot be accessed directly. Instead, 'compliance copies' of Teams chats and channel messages are stored in the 'TeamsMessagesData' hidden folder in Exchange Online mailboxes.
  - Copies of Team chats and private channel messages are stored in personal mailboxes.
  - Teams channel messages are stored in Microsoft 365 Group-linked mailboxes.
  - According to the e-Book, 'Office 365 for IT Pros' (April 2025 edition), compliance copies are not 'perfect replicas' of the original Teams message. They include most of the content, stored as a set of MAPI<sup>33</sup> properties that can be viewed, but do not include either (a) user reactions to chats, such as a heart or smile, or (b) videos for the one-minute long audio messages sent from mobile clients or chat.
  - When a Teams chat or channel message is permanently deleted as a result of a retention policy setting, the system first deletes the compliance copy in the mailbox and then deletes the copy in the Azure Cosmos database.
- Digital content created in SharePoint and OneDrive is stored in two locations:
  - All metadata and list-based content is stored in a dedicated **Azure SQL Content Database** (DB). This Database holds the 'map' required to locate and reassemble the actual content described as binary large objects ('blobs') that is stored in a dedicated Azure File Storage area, as well as the keys needed to encrypt and decrypt those blobs. It also includes checksums for each file stored.
  - All files and digital objects stored in a library are stored in a dedicated instance of **Azure File Storage**. SharePoint uses append-only storage and all content is stored as encrypted read-only binary large objects, or 'blobs'. Any new version of an object creates a new read-only blob.<sup>34</sup>

<sup>33</sup> Messaging Application Programming Interface. This is a technology developed by Microsoft to let applications work with email messages and messaging data. **See:** [What is MAPI? - Mail Server | AccuWeb Help Center](#) (accessed 2 May 2025)

<sup>34</sup> **Sources:** [Introduction to Blob \(object\) Storage - Azure Storage | Microsoft Learn](#), [SharePoint and OneDrive data resiliency in Microsoft 365 - Microsoft Service Assurance | Microsoft Learn](#), [Encryption for SharePoint and OneDrive, Microsoft Teams, and Exchange - Microsoft Service Assurance | Microsoft Learn](#) (accessed 2 May 2025)

## Part 4 – Configuring Microsoft 365 and SharePoint Online to manage records

There are hundreds of configuration settings across the various Microsoft 365 admin centres. Some of these settings can be set in different parts of the same, or different, admin centres. The settings in the table below are only those that are relevant to or specific to the management of records.

### Exchange Online admin

Exchange Online personal or Group-linked mailboxes may contain the only copy of records created or received by a public office. The mailboxes of senior staff or executives are very likely to contain records of higher value to the public office.

**Note:** It is not best practice to rely on mailboxes as a recordkeeping system. State Records NSW's preference is for emails to be captured into a recordkeeping or other business system where authorised minimum retention periods can be applied and implemented, including emails that are part of a record that is required as State archives. Where this has not been done the emails will need to be retained until the minimum retention periods from the relevant retention and disposal authority have been met. Public offices may need to retain the emails of senior staff, executives and other staff with high-risk delegations on an ongoing basis until it is confirmed that emails that document an action or decision have been captured into a recordkeeping or business system that can manage the records for the minimum retention periods required.

Unless some form of retention is set, all personal mailboxes will be automatically deleted 30 days after a user account is deactivated, which could result in unauthorised disposal of records under the State Records Act. IT departments have used various methods since email was introduced to the workplace to retain access to mailboxes.

- Backups (to support disaster recovery and business continuity purposes).
- Converting mailboxes to shared mailboxes.
- Applying litigation hold to entire mailboxes.

None of these options meet minimum recordkeeping requirements to retain records for minimum periods and then appropriately dispose of the records. In most cases they result in open-ended retention and then uncertain and often undocumented disposal actions. Legal holds set in Purview provided a better way to put a hold on specific content in, rather than entire, mailboxes.

See below for details of the suggested retention policy configuration for Exchange Online mailboxes, details of the legacy Messaging Records Management (MRM) functionality now located in Purview, and the ability to create legal holds via Purview.

## Microsoft Entra

Configuration settings in Microsoft Entra that can affect the management of records.

Setting location	Recommended setting	Rationale
<b>Groups – Group settings – General – Microsoft 365 Groups</b>	Set to 'No'.	To stop the uncontrolled creation of Teams and Group-based SharePoint sites.  Note: Changing this setting to no means that organisations must establish an internal process for end users to request the creation of new Teams and SharePoint sites.
<b>Groups – Group settings – Expiration</b>	Subject to an assessment of risk, enable expiration only for 'Selected' Microsoft 365 Groups that are known to contain only facilitative records that may be destroyed under Normal Administrative Practice (NAP). <sup>35</sup> The selected Groups must be listed individually.	Provides a way to remove Groups that are known to contain low-level content. However, if no retention policies or labels are in place, this setting could potentially result in the automatic destruction of records which may be unlawful. <sup>36</sup>
<b>Users – User settings – Guest user access</b> or <b>External identities - External collaboration settings – Guest user access – Guest user access restrictions</b>	Set to 'Guest users have limited access to properties and memberships of directory objects'.  <i>(This setting may be changed in either location in Entra)</i>	Limits what external guests can access.
<b>External identities - External collaboration settings – Guest user access – Guest invite restrictions</b>	Set to 'Member users and users assigned to specific admin roles can invite guest users including guests with member permissions'.	Limits who can invite external guests.

<sup>35</sup> See: [State Records Regulation 2024 and normal administrative practice for public offices](#) | NSW Government (accessed 5 May 2025)

<sup>36</sup> Ibid

<b>Conditional access - Policies</b>	Create conditional access policies that limit what end users and external guests can do. For example, restrict access to SharePoint to users in specific geo-locations. They may also be used in conjunction with Information Sensitivity policies to prevent certain actions such as downloading content to unmanaged devices.	Limits what end users and external guests can access and do. Conditional access is described as 'Microsoft's Zero Trust policy engine, taking signals from various sources into account when enforcing policy decisions'. <sup>37</sup>
--------------------------------------	---	---

## Microsoft 365 admin centre

The configuration settings in the Microsoft 365 admin centre relate to or can affect the management of records.

Setting location	Recommended setting	Rationale
<b>Settings – Search &amp; Intelligence</b>	<p>Review 'Query analytics' regularly.</p> <p>Create Acronyms and Bookmarks to help people find content.</p> <p>Consider creating new search verticals.</p>	To help people find the content they are looking for.
<b>Settings – Org settings - Services – Microsoft 365 Groups</b>	Enable (check) both options: 'Let group owners add people outside your organisation to Microsoft 365 Groups as guests', and 'Let guest group members access group content'.	Allows external guests to be a (guest) member of a Group and access Group content including its SharePoint site.
<b>Settings – Org settings - Services - SharePoint</b>	Set to 'New and existing guests'.	<p>The default is 'Anyone' which is too permissive and essentially allows 'anonymous' access to the environment.</p> <p>Note that this control 'flows' down to the SharePoint admin centre – see below.</p>
<b>Settings – Org settings - Services – Microsoft Teams</b>	Enable (check) 'Allow guest access in Teams'.	Allows external guests access to a Team and also allows them to access the Group's SharePoint site unless this is blocked

<sup>37</sup> See: [What is Conditional Access in Microsoft Entra ID? - Microsoft Entra ID | Microsoft Learn](#) (Accessed 2 May 2025)

through the Microsoft 365 Groups setting above.

<b>Settings –Org settings -Security &amp; Privacy -Sharing</b>	Enable (check) ‘Let users add new guests to the organisation’.	Allows end users to add a guest, provided ‘New and existing guests’ (or ‘Anyone’) is allowed.
--	--	---

<b>Settings –Org settings – Organisation profile - multi-tenant collaboration</b>	Allows a multi-tenant organisation to enable users across the tenants to collaborate.
---	---

## Teams admin

The configuration settings in the Microsoft Teams admin centre listed in the table below can affect the management of records.

Setting location	Recommended setting	Rationale
<b>Teams Settings &amp; policies - Teams – Email integration</b>	Enable (check) both options: ‘Users can send emails to a channel email address’. (Default is enabled)	Allows anyone to send an email to a Teams channel, which captures the email (and any attachments separately) into a month/year-based folder under the channel-linked folder in the Documents library of the Teams SharePoint site.
<b>Teams Settings &amp; policies - Teams – Files</b>	Disable (change to ‘Off’) the ability for end users to access third-party file storage systems such as Google Drive or DropBox from Teams.	Reduces the risk that organisational content will be mixed with uncontrolled content.
<b>Teams Settings &amp; policies – Teams settings</b>	Disable (change to ‘Off’) the ability to create private and shared channels.	Each private and shared channel creates a new SharePoint site that can only (by default) be accessed by the person who created the site and anyone in the private channel. Consider establishing an internal process to allow end users to request private or shared channels ‘on demand’; IT can enable this setting for the period required to create the private or shared channel.
<b>Teams Settings &amp; policies – Guest access</b>	Allow guest access in Teams (default is ‘On’).	There is usually no reason to prevent external users from accessing Teams.

Note that settings may also be set from the Microsoft 365 admin centre.

**Teams Settings & policies – Meetings – Meeting settings – Recording & transcription**

Recordings automatically expire. This is set to 'On' by default with a 120-day default retention period, which means the recordings will be automatically deleted after that period unless they are subject to a retention policy.

Noting that Teams recordings are automatically saved to OneDrive. As OneDrive should not be used to store records, if an organisation wants to keep recordings as records, it will need to move or copy them to a SharePoint site.

**Teams Settings & policies – Messaging – Messaging settings**

By default, end users can delete or edit sent messages. These settings can be left 'as is'.

Retention policies provide a way to prevent the permanent deletion of chat messages for a minimum period.

It is possible to recover all versions of a message, including the original and any modified version, through the eDiscovery functionality in Purview.

## SharePoint/OneDrive admin

The following are the recommended settings in SharePoint admin to support the management of records.

Setting location	Recommended setting	Rationale
<b>Policies – Sharing – External sharing</b>	SharePoint: 'New and existing guests'	For SharePoint, provides a level of control that 'Anyone' doesn't provide.
	OneDrive: 'Only people in your organisation'	For OneDrive, removing external sharing discourages end users from storing final version of records in that location and sharing them. Note that this will not stop them downloading and 'sharing' something by attaching it to an email.

---

**Policies – Sharing – More External sharing settings**

Limit external sharing by domain – Unchecked

Limiting sharing by domain is not recommended as it required maintenance of the list and does not prevent end users from downloading and sending the same item via email.

Allow only users in specific security groups to share externally – Unchecked

Additional controls may be applied as required, for example by removing the ability to share externally from any given site.

Guests must sign in using the same account to which sharing invitation were sent - Checked

Removes the ability for a sharing link to be used by others.

Allow guests to share items they don't own - Unchecked

Removes the ability to on-share content.

Guest access to a site or OneDrive will expire automatically after this many days – 60 (default)

Minimises the risk of granting open-ended access to content.

People who use a verification code must re-authenticate after this many days – 30 (default)

Increases security.

**Policies – Sharing – File and folder links**

Specific people (only the people the user specifies).

Limits sharing to specific people rather than 'anyone'.

May be changed to edit if required.

Choose the permission that's selected by default for sharing links – View

(If 'Anyone' remains the default external sharing choice - Choose expiration and permission options for Anyone links – These links must expire within this many days: 30. Files – View and edit. Folders – View, edit and upload).

**Policies – Sharing – Other settings**

Show owners the names of people who viewed

These are the default options; no change is suggested.

---

	<p>their files in OneDrive – Checked</p> <p>Let site owners choose to display the names of people who viewed files or pages in SharePoint – Checked</p> <p>Use short links for sharing files and folders -Checked</p>	
<b>Policies – Access Control – Unmanaged devices</b>	<p>Set to ‘Allow limited, web-only access’ unless public offices do not manage all devices</p> <p>(Alternatives are ‘Full access’ (default) and ‘Block access’)</p>	<p>Allowing limited, web-only access for unmanaged devices will help to protect records from being downloaded to those devices. However, as not all devices will be managed, the alternative of ‘Full access’ may be required in some public offices.</p>
<b>Policies – Idle session sign out</b>	<p>Do not use, defunct option.</p>	<p>Use the Microsoft 365 admin option in conjunction with Group Policy Object (GPO) settings for devices.</p>
<b>Policies – Network location</b>	<p>Leave ‘Off’</p>	<p>There is usually no reason to enable this setting.</p>
<b>Policies – Apps that don’t use modern authentication</b>	<p>Set to ‘Block access’</p>	<p>There is no reason to allow access.</p>
<b>Policies – OneDrive access restriction</b>	<p>Set to ‘Off’</p>	<p>There is usually no reason to enable this setting.</p>
<b>Settings – Page creation</b>	<p>Set to ‘On’</p>	<p>Default setting.</p>
<b>Settings – Site creation</b>	<p>Uncheck ‘User can create SharePoint sites’</p>	<p>Control site creation.</p>

	<p>Ensure the default time zone is correctly set</p> <p>(After setting the site storage limits to Manual), set the default storage limit for new sites to 500 GB (or as decided by the public office)</p>	<p>Good practice often overlooked.</p> <p>The default storage size is 25 TB. This is too big. Setting to a smaller size provides a way to monitor site growth; storage can always be increased.</p>
<b>Settings – Site storage limits</b>	Set to 'Manual'	Manual is better practice and allows the default size to be reduced and managed as required.
<b>Settings – Retention (OneDrive)</b>	Change to '90 days' (default is 30)	This limit affects when a OneDrive will be deleted when the account is deactivated. It will not do anything if a retention policy retains the content for longer. See also below for further discussion about OneDrive.
<b>Settings – Storage limits (OneDrive)</b>	Reduce to 200 GB (from 1 TB for E3 and up to 5 TB for E5 licences)	Minimises the size to discourage the storage of records. May be increased per user as required.
<b>Content Services – Term Store</b>	Create taxonomies as required, for example terms from a Business Classification Scheme. These terms can then be used on any SharePoint site.	<p>Supports recordkeeping.</p> <p>As an alternative, use choice columns (or lookup lists) on local sites where the choice of options is more suited to a local site than a global list.</p>
<b>Content Services – Content Types</b>	Create global content types as required.	<p>Supports the standardisation of metadata use across an organisation.</p> <p>Two potential negatives: (1) Each content type has to be implemented on each library where it is to be used, which can be a cumbersome exercise. (2) End users may push back on having to use content types, especially if they work from Teams or File Explorer.</p>

Also note that the 'Classic Settings page' accessed via SharePoint admin Settings includes the option to allow the creation of sub-sites. The option 'Disable subsite creation for all sites' should be selected.

See below for details of the retention policy configuration for classic and communication sites, and OneDrives.

## SharePoint and OneDrive advanced management (requires additional licencing)

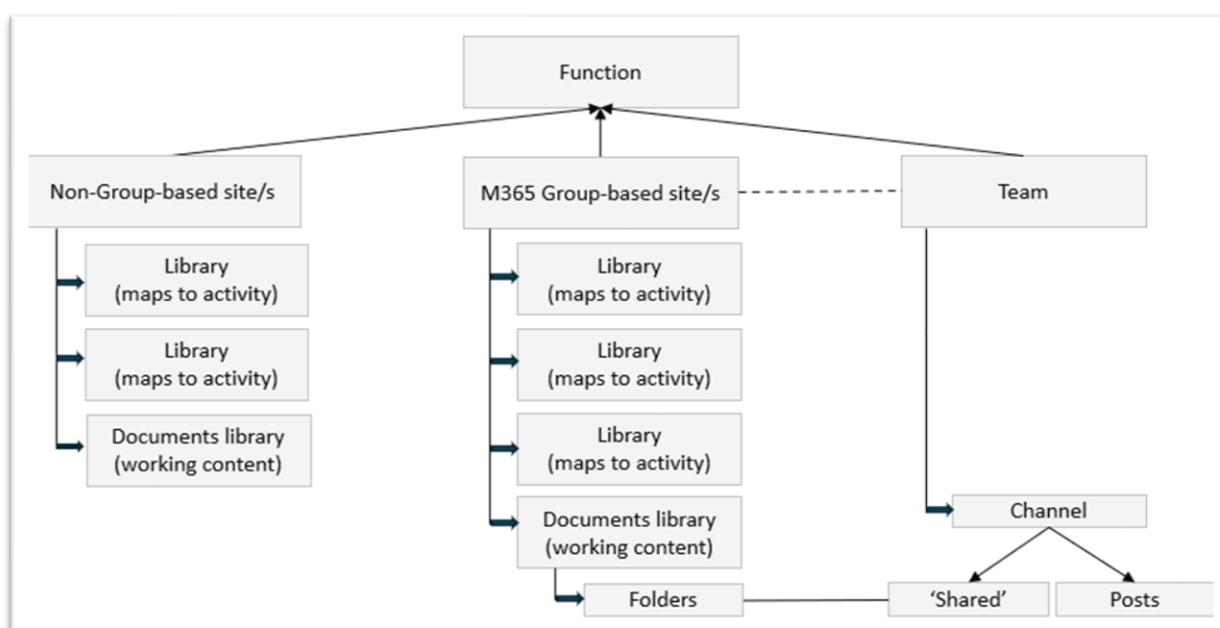
None of the following options are defined here but should be if they are used. For more information, see this link: [Microsoft SharePoint Premium - SharePoint Advanced Management overview - SharePoint in Microsoft 365 | Microsoft Learn](#) (accessed 2 May 2025)

Setting / option	Is this option used or set?	Rationale
Block download policy for SharePoint and OneDrive		
Change history (changes made to a particular site or organisation setting)		
Conditional access policies for SharePoint and OneDrive (to control access based on location or operating system)		
Data access governance reports (for details of potential oversharing and sensitive files)		
Default sensitivity labels for document libraries		
OneDrive access restriction		
Recent actions (review recent site changes)		
Site lifecycle management (to automate tasks across the lifecycle of sites)		
Site-level access restriction (to restrict access to specific SharePoint sites and content)		

## Part 5 – Architecture approach for managing records in SharePoint

Microsoft recommends that organisations should ‘... plan to create one (SharePoint) site for each discrete topic, task, or unit of work’.<sup>38</sup> This usually means that organisations will have many sites.

The guidance in this document follows a similar principle - each site (containing records about a discrete topic, task or unit of work) should map in most cases to a single function with multiple libraries mapped to activities, or a site that maps to a single function/activity pair.



**Image:** The image shows how multiple sites may map to a function, and how records relating to specific activities should be aggregated in libraries using a limited set of folders. The generic ‘Documents’ library included in every site is also included for reference as it is the folders in Microsoft 365 Group-linked libraries that appear in the ‘Shared’ (formerly ‘Files’) tab of every Team’s channel.

This approach assumes (and recommends) that public offices wanting to manage records in SharePoint will implement a controlled approach to the creation of new SharePoint sites and Teams, one that includes records managers in the approval and configuration stages.<sup>39</sup>

<sup>38</sup> **Source:** [Introduction to SharePoint information architecture - SharePoint in Microsoft 365 | Microsoft Learn](#) (accessed 2 May 2025)

<sup>39</sup> It is recognised that, especially since early 2020, many public offices allowed end users to create new Teams that resulted in the proliferation of many SharePoint sites. Public offices may have to establish a process to review these sites and destroy them after a review of their content. The destruction of any records found on these sites, and the sites, must be approved and documented.

## OneDrive is a SharePoint service

OneDrive is a 'personal' SharePoint service ('my.sharepoint.com' in the URL). It should not be used to store records of any kind but in practice many public offices have replaced the former 'home' drives accessed via File Explorer with OneDrive synced to File Explorer so it looks the same to end users. This means that end users may be storing content on File Explorer, unaware that this content is being copied to their OneDrive.

Public offices should develop a policy outlining the use of OneDrive and how content stored there will be subject to retention and disposal actions. See also the suggested retention policy for OneDrive below.

## Guiding principles

For recordkeeping purposes, public offices should create SharePoint sites or Teams that:

- Store content relating to the same business function. Storing records relating to different functions in the same SharePoint site (including Teams-linked SharePoint sites) should be avoided.
- Have the same inherited access controls set at the site level (for Microsoft 365 Group sites and Teams, the Group's membership), inherited by every library or list, folder and document. Where required, some content may be restricted to a sub-set of the site level permissions using unique permissions. Any sharing will extend existing permissions.
- Have the same retention period for all content.

Mixing the above three elements in the same site is likely to complicate the management of records over time. For example, when each channel in a Team is used to store content with different access controls or retention requirements, or when additional folders are added to existing channel-linked folders to do the same thing.

It is recognised that in some cases, organisations may have a requirement to store content relating to several functions in the same SharePoint site. In this case, it is recommended to create additional libraries to store (aggregate) content relating to the same business function. Each of these libraries may be subject to different retention requirements, including using retention labels.

## SharePoint site types

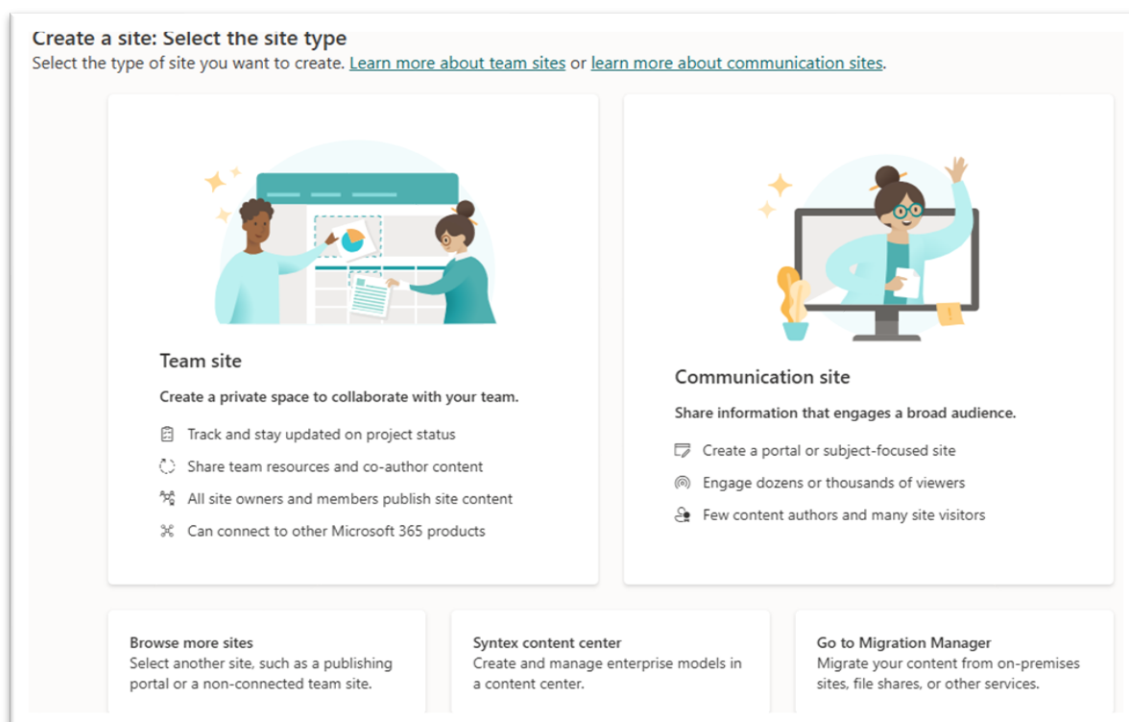
Every SharePoint site is based on one of several pre-defined layouts known as templates. The two most common site type templates since SharePoint was released in 2001 have always been:

- The 'publishing' site template. This template is typically used to publish information on pages, such as on an intranet site. In SharePoint Online, this is a communication site.
- The 'team' site template. This template is typically used to store documents in document libraries and is generally known as a 'team site'.<sup>40</sup> In SharePoint Online, most team sites will be based on a Microsoft 365 group, with some or many of these sites linked with a Team.

---

<sup>40</sup> Somewhat confusingly, every Team in Microsoft Teams uses the Group's team site – the Microsoft Team Team's team site.

Confusingly, *design* templates may also be added to these site templates, so the term 'site template' may refer to either the design template or the site type template. In this document, it refers only to the site type template.



*Image: The two primary options to create a new SharePoint site*

The two primary site type templates that can be created in SharePoint Online, as shown in the screenshot above from the SharePoint admin centre, as well as at least one other site type template that may be used for specific types of records, along with their 'back-end' names<sup>41</sup> are:

- Group-based Team site template ('GROUP#0'). This site type is now the most common and is the site type created when a new Team is created.
- Communication site template ('SITEPAGEPUBLISHING#0').
- Non-Group based Team site templates ('STS#3').

There should be no reason to create any other site type template in SharePoint Online.<sup>42</sup>

After each site is created, a 'look and feel' *design* template may be applied to the site.

## Value and risk

Requirement 2.2 of Principle 2 of the Standard for records management states that public offices should identify high risk and/or high value areas of business and the systems, records and information needed to support those business areas. Requirement 2.3 adds that records and information is a design component of all systems and service environments where high risk and/or high value business is undertaken.<sup>43</sup>

<sup>41</sup> These 'back-end' template names can be seen by right-clicking on any SharePoint page, selecting 'View page source', then searching for 'webtemplateconfiguration'.

<sup>42</sup> See: [Create a team site in SharePoint - Microsoft Support](#) (accessed 5 May 2025)

<sup>43</sup> See: [Principles of records management | NSW Government](#) (accessed 5 May 2025)

With a significant uptake in use of and migrations to the cloud, many organisations now store an ever-increasing volume of content in SharePoint, including via the ‘Files’ tab in Teams.

Public offices should determine the relative level of value and risk associated with the records stored, or that will be stored, in SharePoint. The following is a guide to site creation based on the value and risk associated with the records stored in it.

Assessed value	Suggested site type and anticipated access method	Recommended approach
<p><b>High value, vital, long-term or permanent, sensitive and high-risk records, including those with a minimum retention period exceeding 15 years in a retention and disposal authority</b></p>	<p>Modern, non-Group site (STS#3) for content classified PROTECTED or above. Access via browser only.</p> <p>Group-based sites (GROUP#0) used to store content classified OFFICIAL or OFFICIAL: Sensitive, subject to an assessment of the risk of inadvertent or deliberate changes to access via Group membership, or Teams membership if a Team is connected.</p>	<ul style="list-style-type: none"> <li>• Create dedicated SharePoint sites to store records relating to a single business function, with any required additional security controls and metadata.</li> <li>• Create dedicated activity-linked libraries to store records relating to a specific subject (as indicated in the RDA) for a logical period (e.g., per year, for example ‘Meetings 2024’). This will also facilitate the eventual transfer of records required as State archives to Museums of History NSW</li> <li>• Use folders sparingly, to a maximum of three levels. If there are more than three levels, create new libraries to store the content. For example, a library named ‘Meetings’ might have the following folders: YEAR – MONTH – MeetingDate – Minutes. In this case, create a new library named ‘MeetingsYEAR’ and move the relevant content to that library. This will facilitate the eventual appraisal and disposal actions.</li> </ul>
<p><b>Records to be retained for anywhere from 5 to 15 years in a retention and disposal authority (and then destroyed)</b></p>	<p>Group-based (GROUP#0) or non-Group-based (STS#3) subject to an assessment of the risk of inadvertent or deliberate changes to access via Group membership, or Teams membership if a Team is connected. Access via browser, Teams, mobile device.</p>	<ul style="list-style-type: none"> <li>• Create dedicated SharePoint sites to store records relating to a single business function or capital project.</li> </ul> <p>- These sites will usually be based on a Microsoft 365 Group and Team.</p>

---

Syncing/Add shortcut to OneDrive allowed.

- Create dedicated activity-linked libraries to store records relating to a specific subject, ideally for a logical period. This will facilitate the eventual disposal of the records.
- For projects (including those linked with a Team), the default Documents library may be used with other libraries as necessary.
- Use folders sparingly, to a maximum of three levels. Follow the guidance for folders for high value records in the previous row, where appropriate.

**All other short-term temporary records, including records that are subject to Normal Administrative Practice**

Group-based (GROUP#0). Access via Teams, File Explorer, mobile device.

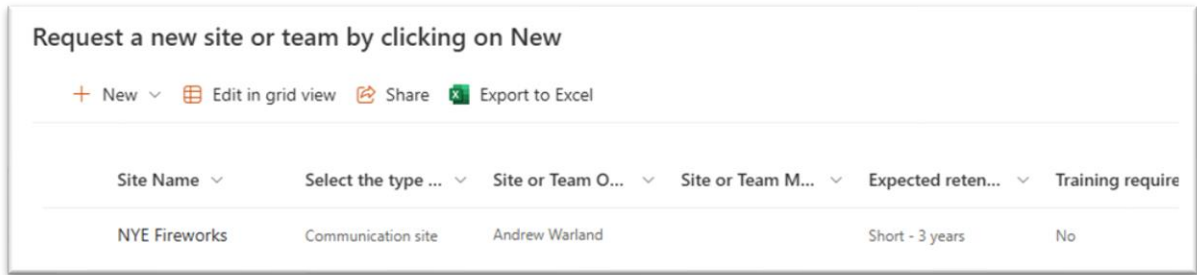
Syncing/Add shortcut to OneDrive allowed.

- Ideally, create SharePoint sites or Teams to store records relating to a single business function or capital project. These sites may be based on a Microsoft 365 Group/Team.
- Use the default Documents library to store and manage records, using folders to separate content as necessary.
- In most cases, the entire site will be reviewed after it becomes inactive and then subject to the required disposal actions.

## Requests for new SharePoint sites and Teams

In a controlled environment where end-users cannot create sites or Teams, the creation of new SharePoint sites (or Teams as these include a site) will need to be based on a formal request (linked to an IT ticket) that, when approved, will then be subject to a provisioning process to ensure they are configured to meet recordkeeping requirements.

An effective way to capture the details in a request is via a SharePoint list on a dedicated site. A link to the list, or to create a new item in the list, can then be copied to any other location. For example, the intranet may include a link to 'Request a new SharePoint site or Team', which will create a new item on the list directly.



*Image: A list presented on a SharePoint page, allowing end users to click +New to request a new site or team.*

When the user clicks on +New, they would be presented with a form as shown in the image below.

The screenshot shows the 'New item' form in SharePoint. The form has the following sections and fields:

- Site Name \***: A text input field with the placeholder 'Enter value here'. Below it is a red error message: 'You can't leave this blank.' and a hint: 'Enter suggested site name'.
- Select the type of site you need**: A dropdown menu with the selected option 'Site with Group and email'. Below it is a hint: 'Default is Group-based site, includes email address'.
- URL Name**: A text input field with the placeholder 'Enter value here'. Below it is a hint: 'Up to 15 characters only'.
- Site or Team Owners**: A text input field with the placeholder 'Enter a name or email address'. Below it is a hint: 'Responsible for the Team and or Site'.
- Site or Team Members**: A text input field with the placeholder 'Enter a name or email address'. Below it is a hint: 'These people have access to the Team and edit rights on the Site'.
- Expected retention**: A dropdown menu with the selected option 'Short - 3 years'.

*Image: An example form to request a new SharePoint site or Team*

The user input element of a SharePoint list can also be presented as a form by selecting the 'Forms' option in the list menu.

### Request a new Team or SharePoint site

Hi Andrew Warland, when you submit this form, the owner will see your name and email address

@onmicrosoft.com

Site Name \*

Enter value here

Site purpose

Enter value here

Select the type of site you need

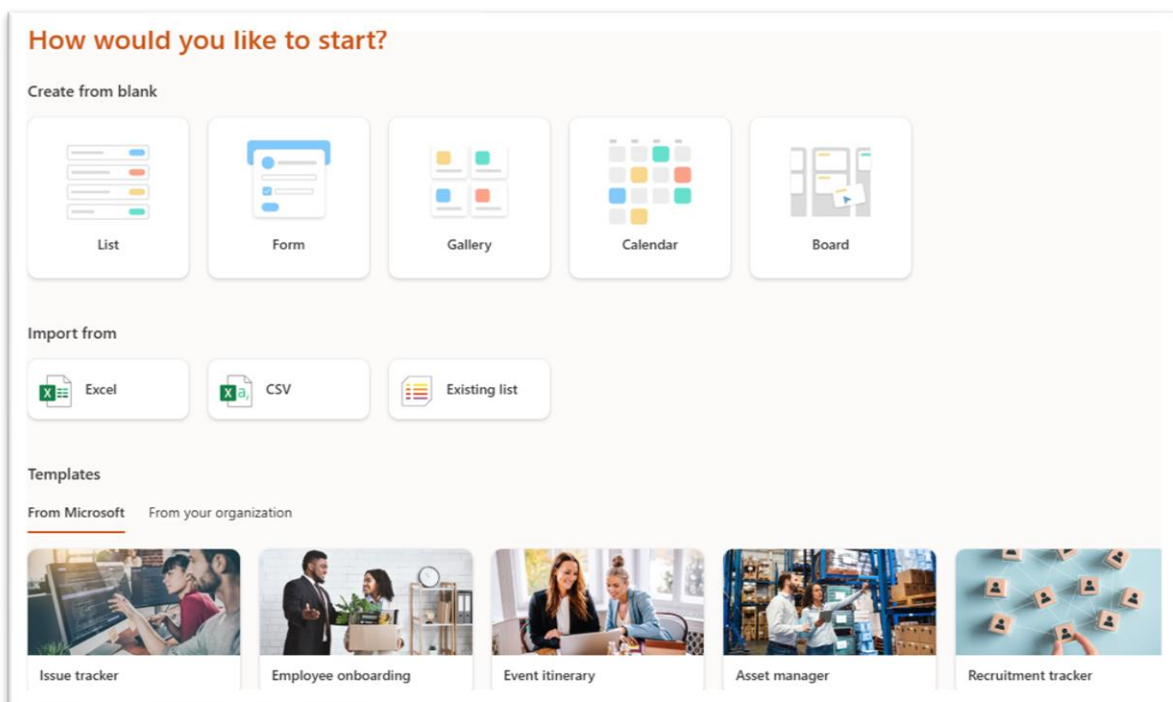
Site with Group and email

URL Name

Enter value here

*Image: The forms-based view of a request for a new SharePoint site or Team*

A new list can be created from the front page of any SharePoint site ('+New' option). The options to create a new list are shown below.



*Image: Options to create a new list in SharePoint, including from a template*

Additional columns may then be added to any list, even those created from a template. For example, the list could be used to record details of the function each site maps to, its status (e.g., active, inactive, deleted), when it was destroyed, and so on.

Requests for new sites or Teams could include the following questions:

- IT ticket number reference (if any)

- What is the purpose of the site or Team?
- Will the site or Team be used to create or capture records? (If yes, then the request should be reviewed by a records manager)
- If a site without a Team is required, what type? (default is Group-based, alternatives are non Group-based site and communication site)
- What is the business function? (Ideally a choice option)
- What is the preferred site/Team name? (4 to 20 characters, CamelCase, no spaces)
- What is the preferred site/Team display name?
- Who will be the site or Team owners? (2 or 3 only)
- (Optional) Who will be the site or Team members? (May be added by the Site/Team owners later)
- (Optional) Are any other permissions required? (e.g. access and security, records are Read-Only, etc.)
- Are any additional libraries or lists required? (Free text response, this may help determine the types of records that may be created, mapped to activities and RDA classes if required)
- Is any additional metadata required? (Free text response)
- Are any content types required?
  - A clue to this question may be in the need for additional metadata in the previous question. If additional metadata is required, it may be useful to create them as site columns and add them to a site content type.
- Are document sets required?
  - Document sets are usually recommended instead of folders for sites that are used to group records in a library relating to a given matter and need specific metadata at the 'grouping' level. For example, staff files, client agreements, tender processes, recruitment activity.
- What is the expected retention for the content? (Free text response to help determine the RDA classes)
- Is any training required?
- Any other comments?
- (Requestor's name and business area if not automatically captured).

The following columns should be added to help keep track of each site.

- External sharing (enabled or disabled)
- Storage
- Hub relationship
- Sensitivity
- Status (e.g., Active, Inactive, Deleted)
- Deleted (date)
- Deletion approved by

## Provisioning new SharePoint sites

Once approved, a site (or site linked with a new Team) can be created and provisioned as described below.

## Feature / option

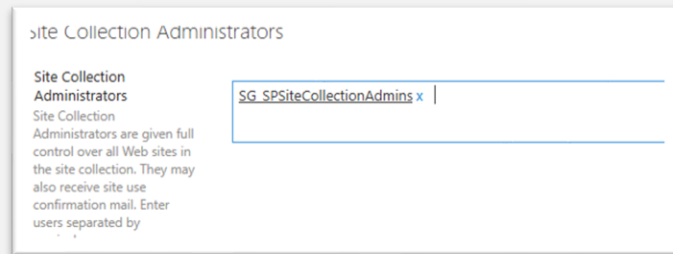
## Recommended setting

### Site Collection Administrators

The Site Collection Administrators will always be (a) the SharePoint admins, and (b) records and information managers responsible for managing records on a site. These may be combined into a single Security Group applied to a site.

Add a pre-defined Security Group that includes both SharePoint admins and all records and information managers.

Note: If a Group-based site or a Team is created, the Group/Team Owners group will be automatically added to the Site Collection Administrators area. Public offices should remove the Group Owners from this area to minimise the potential for unauthorised changes made by site owners to the Site Collection Administration settings of each site and replace that group with Security Group, as shown in the image below. The Group Owners will still be Site Owners (next option).

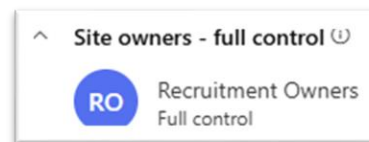


### Site Owners

The Site Owners usually consist of two to three people working in a business area or working on a project or similar type of 'group' function, who have primary 'ownership' of the site. Site Owners may create new libraries and lists, as well as pages, as required.

As shown in the request.

Note: If a Group-based site or a Team is created, the Group/Team owners group will be automatically added to the site owners permission group (example in image below). There is no requirement to also add end users by name.

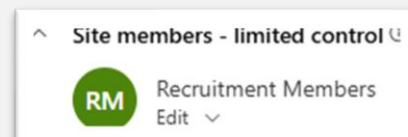


### Site Members

Site Members have 'add/edit' rights on the site, allowing them to create and modify libraries and lists and edit existing content.

As shown in the request, but Members (and any Visitors) will usually be added by the Group/Team or Site Owners.

Note: If a Group-based site or a Team is created, the Group/Team members group will be automatically added to the site members permission group (example in image below). There is no requirement to also add end users by name.



---

**Site Visitors**

As required.

Site Visitors have read-only access to the site. Adding them here is optional.

**Document ID feature**

This feature provides a way to meet the minimum metadata requirement for a unique ID.

Site Settings – Site Collection Administration – Document ID feature: Activate

Site Settings – Site Collection Administration – Document ID settings. Configure the Document ID prefix with 4 to 12 characters that are the same or very similar to the URL of the site, as shown in the example image below where the site URL name is ‘FINANCEAP’.

**Document Sets feature**

This feature should be activated even if it is not used.

Site Settings – Site Collection Administration – Document Sets: Activate, even if not used.

**SharePoint Viewers feature**

This feature allows end-users of a site to see who has viewed content in a SharePoint library.

Site Settings – Site Actions – SharePoint Viewers: Activate

**Site Columns**

Site columns provide a way to add additional metadata to libraries and lists on the site.

Create additional site columns as required.

Additional site columns may be required on sites that will be used to store and manage high value, high risk, vital and permanent records and are an effective way to ensure consistency in metadata across a site. Columns may then be added to document libraries and lists as required, rather than adding them directly on each library or list.

**Site Content Types**

Site content types provide a way to control the metadata added to documents and document sets in a library.

Organisations may also use global content types.

Create site content types as required.

Note that some Content Types may be created in the Content Type hub in SharePoint admin but are more likely to be created and deployed in specific sites rather than every site.

## Regional Settings

Site Settings – Site Administration – Regional Settings. Check to make sure that the time zone is correct, and the ‘Locale’ is set to English (Australia). Otherwise, dates will appear in the US format of MM/DD/YYYY.

## Custom features

Some sites may include custom features or apps that need to be enabled. For example, Search PnP.

# Configuring individual SharePoint sites to manage records

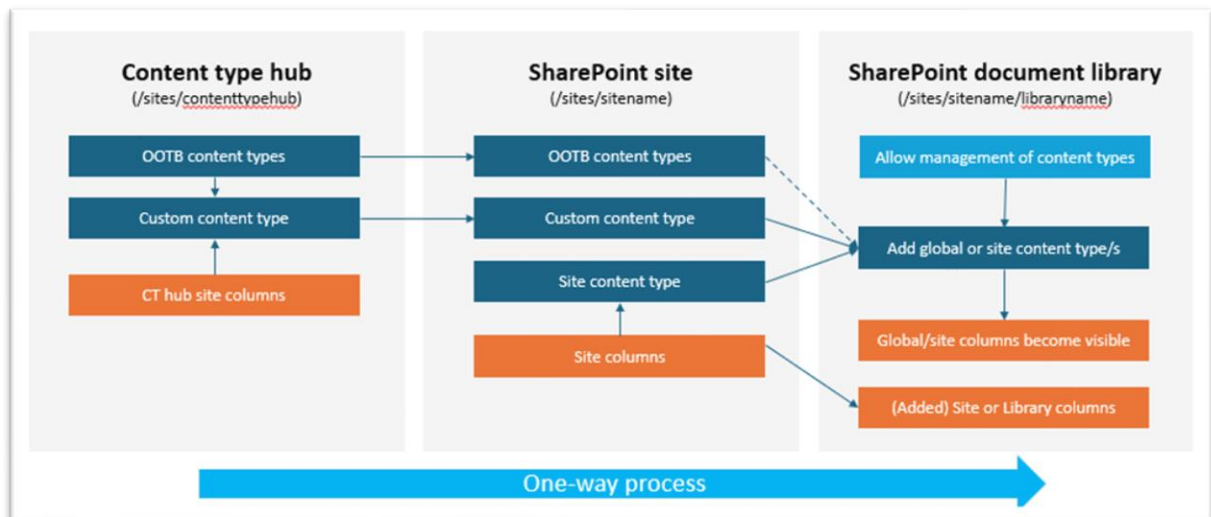
Sites that will be used to manage records should be configured as described below after they are created and provisioned.

## Site columns (metadata) and content types

All new SharePoint sites include over 150 ‘out of the box’ metadata columns (fields). These include the minimum metadata requirements of Agent (‘Created by’ and ‘Modified by’) and Date (‘Created’ and ‘Modified’).

Additional metadata columns may be created:

- In ‘global’ content types created in the Content Type hub. These content types may then be applied to individual libraries via the library settings in a site.
- As site columns in individual sites, then added directly to a library or via a content type created at the site level with those columns included. This is the preferred option on SharePoint sites where additional metadata is required and that metadata may be used in multiple libraries or lists.
- As library or list columns in sites. These columns are only available in the library or lists where they were created.



Adding a global or site column to a library is a one-way process. Any changes made to the column at the library or list level, for example to add or modify choice options, do not 'flow upwards' to the original global or site column.

**Note:**

- The requirement for a unique ID can be met through the activation and configuration of Documents IDs as noted above. When the Document ID feature is activated, the 'Document ID' column will be available in any library view.
- The use of retention labels and information sensitivity labels in a library automatically adds the 'Retention label' and 'Sensitivity' columns.
- The use of the 'out of the box' option to 'Request sign off' automatically adds the 'Sign-off status' column to the library view. Other columns may also appear in libraries or lists when workflows are added.

Public offices that create and capture permanent value records must ensure that these records will have the appropriate metadata to facilitate their eventual transfer to Museums of History NSW as State archives. The best way to ensure this is to aggregate permanent value records in libraries, with all the metadata that may be required.

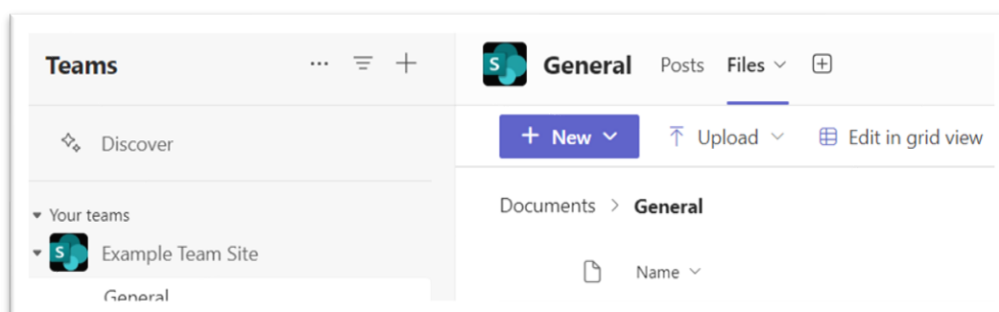
Additional site columns may be created and applied to records in any site, based on minimum metadata requirements for metadata and any business requirements.<sup>44</sup>

## Create activity-based libraries to aggregate related records

SharePoint document libraries are a logical and practical way to aggregate records relating to the same activity. This is because all the metadata is set at the library level. Each SharePoint site can have up to 2000 libraries.

- Folders should be limited to two levels.
- When folders reach three or more levels, that is often a sign that a new library should be created.

It is recognised that aggregating records in dedicated libraries may not always be suitable or practical, especially for short-term temporary records where folders in the generic Documents library of a site map to channels in a Team via in the Files tab, as shown in the image below.



**Image:** The 'General' channel maps to the 'General' folder in the Documents library of the SharePoint site linked to the Team.

<sup>44</sup> See: [Minimum requirements for metadata for authoritative records and information | NSW Government](https://www.nsw.gov.au/nsw-government/recordkeeping/create-and-capture/using-metadata) (accessed 5 May 2025) and <https://www.nsw.gov.au/nsw-government/recordkeeping/create-and-capture/using-metadata>.

The following is a guide to when new libraries should be created.

Mandatory	Recommended	Optional
<p>Sites (typically not linked with a Team or even a Microsoft 365 Group) that are used to manage records that are high value, vital, long-term or permanent (transfer to Museums of History NSW as State archives), sensitive and high risk.</p> <p>These libraries will usually include additional metadata set at the site or library level.</p>	<p>Group-based sites that are used to manage records that must be retained for anywhere from 5 to 15 years (and then destroyed).</p> <p>These libraries may include additional metadata set at the site or library level.</p>	<p>Project and other sites linked with a Team.</p> <p>Sites use to manage short-term temporary records with a retention period of up to 7 years.</p> <p>These sites will usually use the default Documents library, grouping records by folders, and use the default metadata.</p>

## Configuring document libraries

SharePoint document libraries are the preferred way to aggregate records relating to the same business activity because they contain all the metadata about the records stored in them; this is not possible with folder-based grouping of content.

### Library naming conventions

The name of each library should be kept concise to assist with keeping the overall path of each record to under the maximum limit of 400 characters (including https:// - tenantname - sitename - libraryname - foldername/s - documentname - extension (e.g., docx)<sup>45</sup>.

When creating a new document library or list:

- Limit the library or list name to no more than 25 characters as any more will not be visible on the left-hand navigation of the SharePoint site.
- Use CamelCase or underscores between words. Avoid putting spaces or hyphens between words as these are changed to '%20' in the URL. Spaces between words and hyphens can be added to the display name after the library has been created.
- Use names that are meaningful and relates to the content, and with a year where this is useful as this can help with retention. For example, 'Meetings2024', 'Budget\_20242025'.
- Avoid common or unclear acronyms unless the site name provides the context for them.
- Include a description indicating what the library is about. The description can contain up to 255 characters.

Once the new library has been created, it will appear in the left-hand navigation (unless this option was not selected when the library was created) and be visible from the Site Contents page. The left-hand navigation elements can be removed (not deleted), moved,

<sup>45</sup> The 400 character limit is reduced to 255 characters if end users access the content via File Explorer via the 'Sync' or 'Add shortcut to OneDrive' options. **Source:** [Restrictions and limitations in OneDrive and SharePoint - Microsoft Support](#) (accessed 2 May 2025)

or modified by clicking the 'Edit' option at the bottom of the left-hand navigation pane. Removing libraries or lists from here does not remove them from the Site Contents listing.

### Adding metadata to libraries and lists

As noted above, metadata may be created as site columns, which means they can be added to any library or list. This option is useful if the same metadata is to be used in different libraries or lists on the same site. Custom site columns are only available on the site where they were created.

There are two ways to add additional metadata columns to a library or list.

- By clicking the 'Add column' option in the library or list view. This allows end users to add columns from multiple options such as 'Text', 'Choice', 'Date and Time' and so on. There is also an option to 'Show or hide columns' which can be used to add or remove most columns. Note that the 'Document ID' column cannot be added via this option. Note that this only creates the new column in the library. Use the next option to create columns that can be accessed in multiple libraries.
- By adding new (or existing site) columns. To do this, click on the library, then navigate via the gear icon to Library settings > More library settings. This opens the library settings page. At the bottom of the list of existing columns in the library, click on either 'Create column' to create a new library column, or 'Add from existing site columns' to add an existing site column.

Tips for creating new columns:

- Use Single Line of Text (255 characters) for most text related columns. Only use Multi Lines of Text for more complex text columns including the option to make use of 'Append only' comments.
- Do not use Number columns for any numbers unless they may need to be calculated. For example, don't use the Number column for post codes, telephone numbers and so on. Use Single Line of Text instead.
- If there are more than 20 options in a Choice column, consider using a Lookup list, where the options are contained in a separate list. This can be easier to maintain.
- Use a Choice column instead of the 'Yes/No' column for 'Yes' and 'No' answers. The 'Yes/No' column does not display those words.
- Use the Managed Metadata column to make use of terms in the Term Store.
- Use default values so end users don't have to add them. For example, if a library in a site maps to a specific function and activity, then those values can be set as defaults (Single Line of Text, Choice, or Managed Metadata).

**Note:** It is not uncommon to see duplicate column names in libraries and lists. This usually occurs because someone has added a column before a content type with the same column name was added. Hovering a mouse over the column name in the library settings will show the actual 'system name' for the column. Duplicate column names should be cleaned up as soon as they are detected to avoid issues with how they are used.

### Adding content types to a library

There are two ways to add a content type to a library:

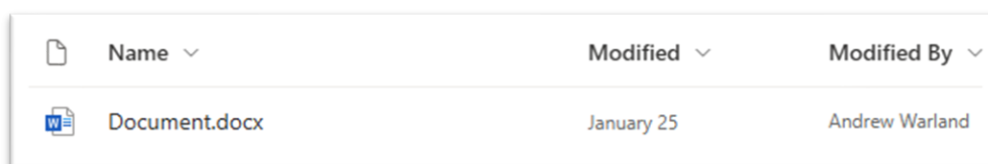
- Via the library view
  - Open the library.
  - At the far right of the list of displayed columns, click 'Add column'.
  - Scroll down to 'Add content type', then click 'Next'.
  - From the drop-down list under 'Choose content type', select the content type to be added.
  - Any columns that were added to the content type will appear automatically in the Columns section of the library settings.
- Via library settings
  - Open the library and from the gear icon navigate to Library settings > More library settings.
  - Click on 'Advanced settings'.
  - Click 'Yes' to 'Allow management of content types'. Click OK at the bottom of the page to save the change.
  - In the Library settings page, a new 'Content Types' section appears.
  - Click on 'Add from existing site content types' to add either global or site content types.
  - Any columns that were added to the content type will appear automatically in the Columns section of the library settings.


After global or site content types have been added to the library, any columns added to those content types will appear automatically in the Columns section of the library settings.

## Library and list views

Every site library (and list) comes with an extensive set of default metadata columns, presented in a default 'All documents' view (or 'All items' for a list). Every view has its own URL address with the extension '/Forms/AllItems.aspx' after the library name. These hyperlinks can then be placed in multiple locations, including in the left-hand navigation bar of a SharePoint site. They may also be shared via email, like any other hyperlink.

When a new library is opened, the default 'All Documents' view displays the following default columns: Icon (e.g. Word), Name, Modified and Modified by, as can be seen in the image below.



Icon	Name	Modified	Modified By
	Document.docx	January 25	Andrew Warland

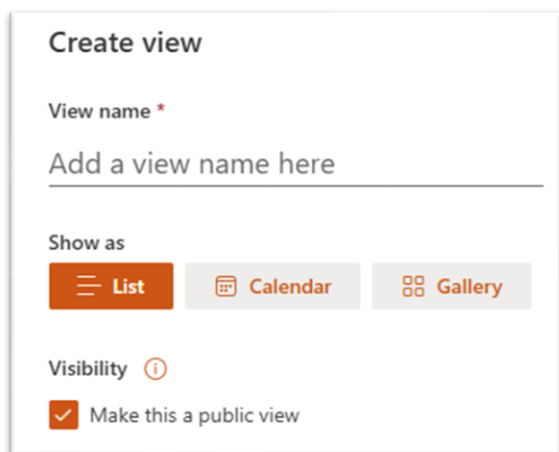
*Image: The four columns that are visible in every default library view*

The metadata that appears in each view can be modified in two ways:

- By clicking the 'Add column' option. This allows end users to create new columns in multiple options such as 'Text', 'Choice', 'Date and Time' and so on. There is also an option to 'Show or hide columns' which can be used to add or remove most columns. Note that not all columns can be added in this way. For example, the 'Document ID' column can only be added via the next option.
- By clicking the down arrow next to 'All Documents' and then clicking either 'Edit current view' or 'Create new view'. Either of these options include a range of

options to add or remove the columns in the view, sort, filter or group columns, and other functionality.

Anyone with edit access to the library can create a new view. Views are by default visible to anyone who has access to the library, but they may be set to private by unchecking the option to 'Make this a public view', in which case only the person who created them (and the site collection administrators) can see them.



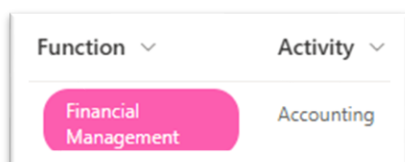
*Image: The 'Create view' option in a SharePoint document library, showing the option to 'Make this a public view' by default.*

Views can be used to create a form of pre-defined standard search. For example, in a document library containing meeting minutes with a 'Document Type' column, a view could present just the Minutes for a given year (filtered by the date range).

As can be seen in the image above, a view can be presented as a Calendar, provided the library or list contains at least two dates usually for short periods typical of a calendar entry.

Some columns may appear only when certain features are used. For example, the 'out of the box' options to 'Request sign-off' and 'Request approval' that are available from the three-dot menu for every document will, when used, add the 'Sign-off status' or 'Approval Status' column to the library. Note: the 'Request approval' option must be enabled before it appears. It links with the Teams approval process which means that all approvals can be viewed from the Teams Approvals app.

Some columns may be formatted in different ways by clicking on the column, then selecting 'Column settings' - 'Format this column'. For example, columns with choices can be formatted to show the choices in different colours.



*Image: Example of the use of colours in a library column*

Document libraries used to store records should display the following minimum metadata elements in at least one view. This metadata can then be used as the basis for disposal processes described below.

- Type (icon)
- Document ID
- Name

- Document Type
- Version
- Modified (date)
- Modified by (agent)
- Function
- Activity
- Retention label (if used)
- Sensitivity (if used)
- Content Type
- Created (date)
- Created by (agent/author) \*
- File size

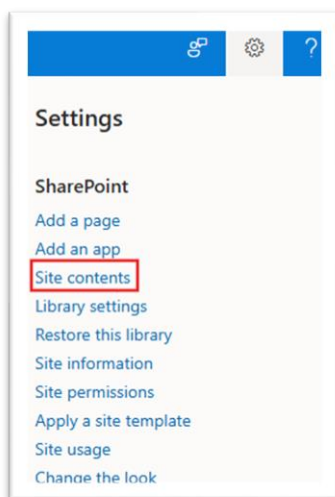
\*The 'Created by' column displays the name of the person who created the item in the library as an original author or the person who added it, not the author of an item that was uploaded.

### Exporting library metadata, including for disposal purposes

The data in the columns listed in a view will be included when the 'Export to Excel' option is selected on any library. The exported metadata may be used to seek approval for the destruction of the records stored in the library.

## Site contents

The Site Contents section of every SharePoint site displays all the libraries and lists on the site. It can only be seen from the browser view of a SharePoint site (e.g., not via Teams, a mobile device, or File Explorer), and is accessed via either (a) the left-hand navigation - 'Site Contents' link or (b) the gear (Settings) option on the top right of the site - 'Site Contents'.



*Image: The 'Site contents' link can be accessed via the gear (Settings) option as shown in the image above.*

The Site contents page shows all libraries and lists that have been created on the site, including five libraries, visible in the image below, that are included with every new SharePoint site. End users with access to the site can see all the libraries and lists unless they don't have access to them.

There are five default libraries that come with every SharePoint site that should never be deleted:

- Documents.
  - When a Group-based SharePoint site is linked with a Team, each channel in the Team creates a folder in the Documents library.
- Form Templates.
  - This library may be used by the system. It should NOT be used to store forms or templates as its name suggests.
- Site Assets.
  - This library is used to store a range of content, including images uploaded to pages and also OneNote.
- Style Library.
  - This library is usually empty but should not be used.
- Site Pages.
  - This library is where all pages, including 'News' pages, are stored.

Contents		Subsites		
Name	Type	Items	Modified	
Documents	Document library	0	7/16/2022 8:01 AM	
Form Templates	Document library	0	7/19/2022 2:39 AM	
Site Assets	Document library	1	7/16/2022 8:01 AM	
Style Library	Document library	0	7/16/2022 8:01 AM	
Site Pages	Page library	1	7/16/2022 8:01 AM	

*Image: The default libraries in every new SharePoint site (including sites linked with a Team)*

If the Site Pages library is deleted, the site will not open from the browser unless an admin restores the deleted library. Deleted libraries can be restored from the Recycle Bin for 93 days.

## Disposal process/stubs

SharePoint does not have the ability to create 'stubs' to show that a record previously existed in a library. The only way to achieve this outcome would be to replace the existing records and all previous versions with a very small document or object. This is not an ideal solution as it will eventually result in inactive sites that contain nothing more than these small documents or objects and their metadata.

It is better practice to export the metadata for the records to be destroyed and, after approval has been obtained for their destruction, store the metadata and the approval in a separate secure location and then destroy the original library and the site if no other content needs to be retained.

## What happens to records and other content that is destroyed?

It is not possible to permanently destroy records in a SharePoint site if the site or individual items stored on the site are subject to a retention policy, retention label, or eDiscovery hold. They may be 'soft-deleted', but they will be captured in the site's Preservation Hold library; this library is accessible only to the SharePoint administrators and Site Collection Administrations.

No-one, not even administrators, can delete content in the Preservation Hold library while that content remains subject to a retention period 'hold'.

When records that are stored in a SharePoint library cease to be subject to a retention policy or eDiscovery hold, the content in SharePoint document libraries (including in the Preservation Hold library) may be permanently deleted, once a copy of the metadata for the records has been captured and approval for the destruction has been obtained.

Deleted items are moved to the site's Recycle Bin where they remain for 93 days. They will then be permanently deleted by a system process.

After the 93-day recycle stage is complete, deletion takes place independently for:

- The item's metadata that was stored in the Azure Content Database.
- The actual content ('binary large object') that was stored in Azure Blob Storage.

According to Microsoft, metadata is removed immediately from the database, which makes the content unreadable unless the metadata is restored from backup. SharePoint maintains 14 days-worth of backups of metadata. These backups are taken locally in near real time and then pushed to storage in redundant Azure Storage containers on a five-to-ten-minute schedule.

When the 'blob' content is deleted, SharePoint utilizes the soft delete feature for Azure blob storage to protect against accidental or malicious deletion. With this feature, there are a total of 14 days in which Microsoft (only) can restore content before it is permanently deleted and 'removed from the service'. The location where the blob was stored is then available to be overwritten.<sup>46</sup>

---

<sup>46</sup> **Sources:** (a) [SharePoint and OneDrive data resiliency in Microsoft 365 - Microsoft Service Assurance | Microsoft Learn](#), (b) [Delete Blob \(REST API\) - Azure Storage | Microsoft Learn](#) (accessed 2 May 2025)

## Part 6 – Compliance in Microsoft Purview

Microsoft Purview includes a range of features and functionality that can be used to manage critical risks and support regulatory and compliance requirements. The following functionality can be used to support the management of records.

- Audit logs
- eDiscovery: Standard and Premium, Content Search
- Data Lifecycle Management: Retention policies and retention labels and label policies, AI and Machine Learning classifiers, Data explorers, Exchange (legacy) Messaging Records Management (MRM) policies
- Records Management (requires E5): File plan-based retention labels, Events, Disposition
- Information Protection: Information sensitivity labels
- Compliance Manager: Includes built-in assessments for ISO 16175, the Standard on records management, and a wide range of other compliance assessments
- Data Loss Prevention
- Communication Compliance
- Insider Risk Management

Purview also includes functionality that supports information security and privacy management.<sup>47</sup>

While Purview includes a range of recordkeeping functionality, public offices will need to develop internal processes and procedures, or consider acquiring third-party applications, to address some gaps, especially:

- The implementation of general retention and disposal authority (GA) retention classes to logical aggregations of records.
- The management of disposal actions at the end of retention, including methods to document what records were destroyed or transferred.

Both points are addressed in this document.

### Audit logs

Audit logs in Microsoft 365 capture an extensive range of activities right across the entire ecosystem. According to Microsoft, '(all) user and admin operations performed in dozens of Microsoft services and solutions are captured, recorded, and retained in your organisation's unified audit log'.<sup>48</sup>

Activities relating specifically to the creation, capture or management of records make up only a small sub-set of the total of audit activity recorded in the logs.<sup>49</sup>

The image below shows the options for an audit log search.

---

<sup>47</sup> For more details, see: [Learn about Microsoft Purview | Microsoft Learn](#) (accessed 2 May 2025)

<sup>48</sup> Source: [Learn about auditing solutions in Microsoft Purview | Microsoft Learn](#) (accessed 2 May 2025)

<sup>49</sup> See this Microsoft page for the full set of activities that are captured: [Audit log activities | Microsoft Learn](#) (accessed 2 May 2025)

*Image: Audit log options*

Audit logs are generally accessible for up to 12 months. Audit logs may be retained for longer if they are subject to an audit retention policy that can be set to any period from 7 days to a maximum of 10 years.

In practice, however, only a relatively small and specific set of audit information is likely to be required for recordkeeping purposes:

- Activities relating to a file (document), site ('website') or library ('folder') in SharePoint
- Activities relating to a specific user

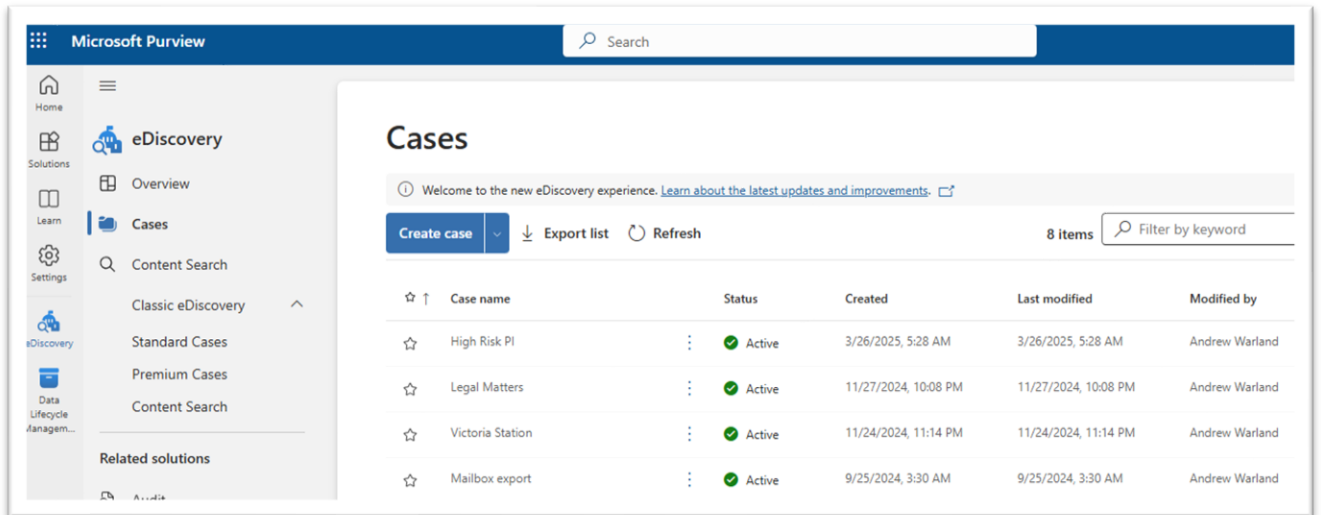
Audit logs relating to a specific site, library or document can be exported as required, including via PowerShell at set time intervals, and then saved to a different location for long-term retention. Exported audit log details are not stored with the individual record they relate to, but in a csv file that can be stored on the same SharePoint site or other location. The only type of audit information that forms part of individual records in SharePoint and OneDrive is the version history that shows who modified a document and when, and any metadata changes.

## eDiscovery and Content Search

The eDiscovery<sup>50</sup> section in Purview has two primary options: Cases and Content Search. The section still shows the 'Classic eDiscovery' options that can be seen in the image below.

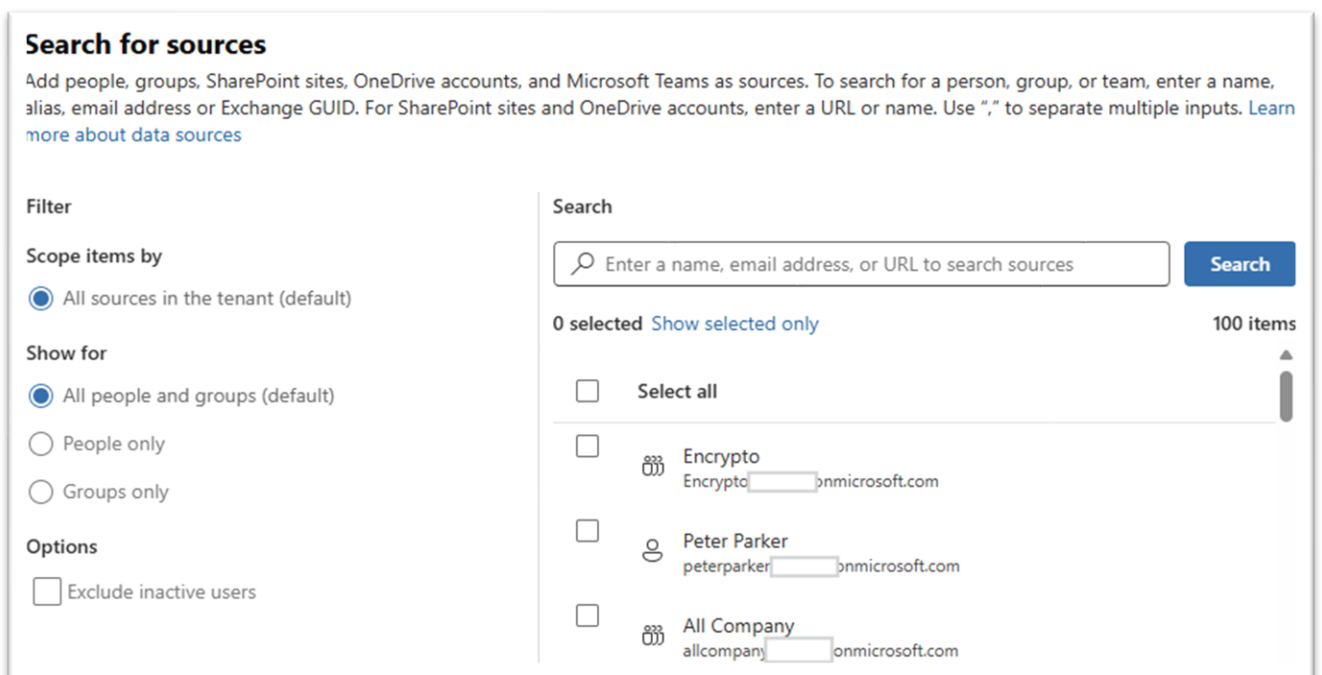
Note that all screenshots below are from the new eDiscovery sections.

<sup>50</sup> For more information about eDiscovery options in Purview, see [Learn about eDiscovery solutions | Microsoft Learn](#) (accessed 2 May 2025)



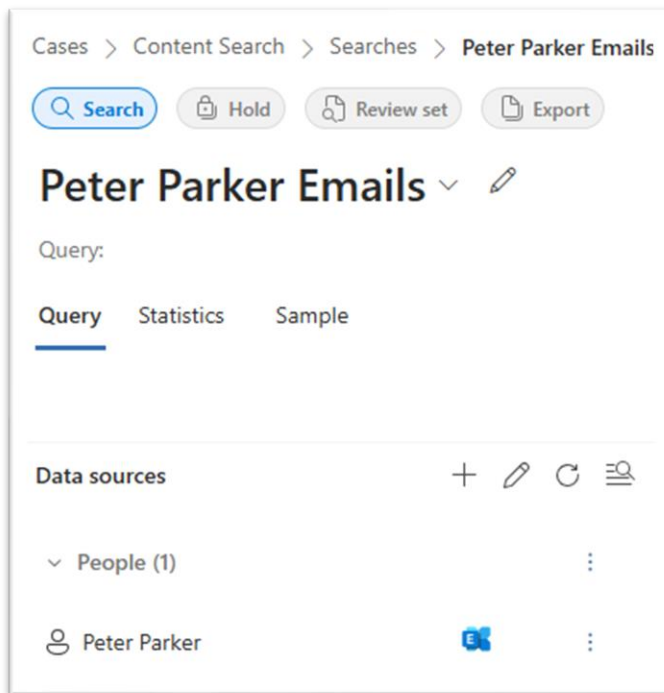
*Image: The eDiscovery options in Purview (May 2025)*

The Content Search option, which also provides the search functionality for the standard eDiscovery option, allows Global Admins and Compliance Admins, as well as eDiscovery Managers, to search for content across all, or select locations in, the primary workloads shown in the image below. The standard eDiscovery option creates a case and includes the ability to place the content on hold.



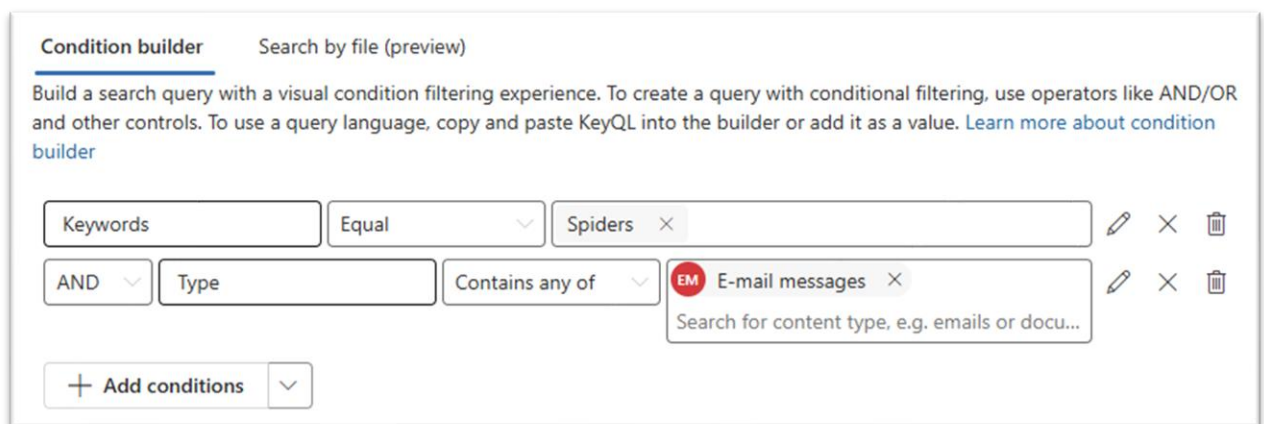
*Image: Content Search scope*

By selecting 'People only', then the individual name (e.g., 'Peter Parker'), the relevant admin may then decide whether to include their mailbox and OneDrive, or, as shown below, just the mailbox.



*Image: Scope for the individual account*

The 'Condition builder' may then be used to look for specific keywords, or to narrow down by date, subject/title, participants and type.



*Image: Condition builder options*

The query is then run. Statistics relating to the search are presented, a sample may be viewed, the content found may be added to a review set, and the content may then be exported.

**Export**

**Messages and related items from mailboxes and Exchange online**

- Include Teams and Viva Engage conversations  
Collect up to 12 hours of related conversations when a message matches a search
- Organize conversations into HTML transcript  
Contextual chat messages will be threaded into HTML transcript for ease of review and handling
- Access links (cloud attachments) in messages  
Collect items from links to SharePoint or OneDrive

ⓘ Including cloud attachments will increase the size and quantity of your exported results.

ⓘ If you have version as shared feature enabled, this will retrieve the version of the document when it was shared. [Learn more about version as shared](#)

Latest version only ▼

**Export type**

Select what you'd like to export. [Learn more about export types](#)

- Export items report only
- Export items with items report

**Export format**

Select how you'd like to format your export. [Learn more about export formats](#)

- Create PSTs for messages
- Create .msg files for messages

*Image: Some of the export results options relating to a mailbox*

## Retention for content in Microsoft 365 – policies or labels?

Requirement 2.5 of the Standard for records management states that records and information management processes must safeguard records, information and data, including records with long-term retention.<sup>51</sup>

In line with the Standard, public offices should understand how retention works in Microsoft 365 and implement a model (after careful planning) that is (a) not complex, (b) protects records from unlawful access, destruction, loss, deletion or alteration, (c) retains records for as long as they are needed, and (d) allows for the systematic and accountable destruction of records when legally appropriate.

Retention and disposal actions for content stored in Microsoft 365 is achieved primarily by implementing retention policies and retention labels to prevent the permanent destruction of selected content for as long as a retention 'hold' applies, including on items that have been 'soft-deleted' by end users. See below regarding options for long-term retention (usually more than 15 years).

The image below summarises the difference between retention policies and retention labels.

<sup>51</sup> See: [Principles of records management | NSW Government](#) (accessed 5 May 2025)

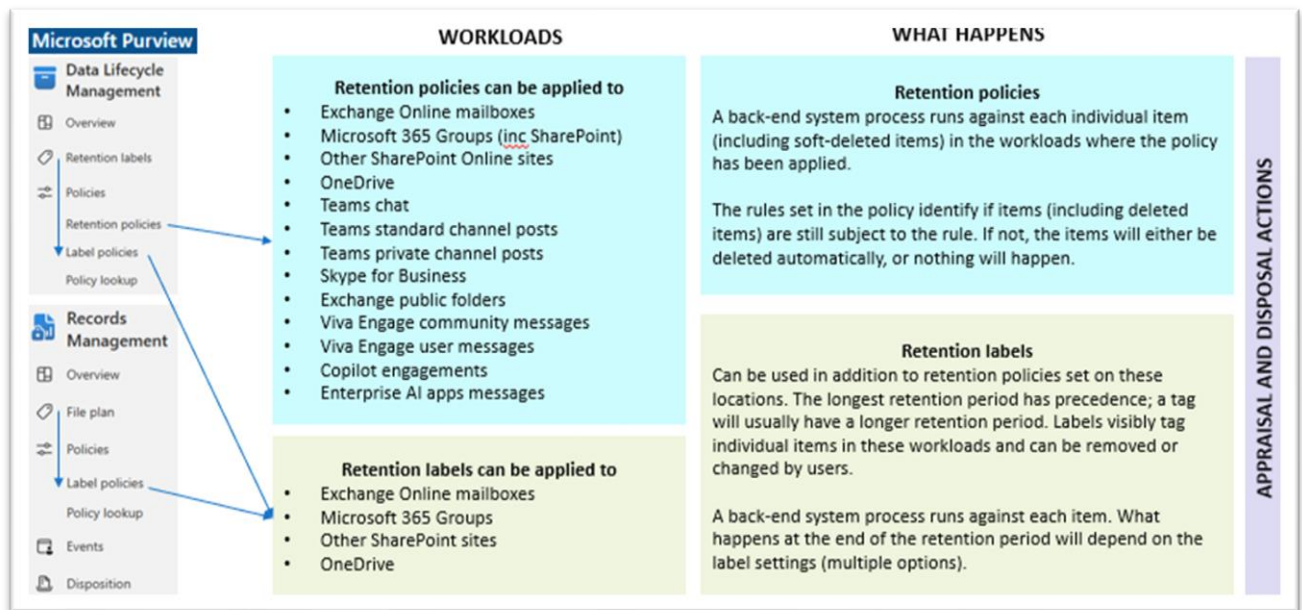


Image: Summary of retention policies and retention labels

## What is the difference between a retention policy and a retention label?

The difference between a retention policy and a retention label is summarised below.

- **Retention policies** work 'behind the scenes' as a 'back-end' system process. They can be applied to all Microsoft 365 workloads shown in the image above.
- **Retention labels** are made available in the required location by being 'published' as label policies. They may then be applied by administrators or users, or via an automated process to individual items in mailboxes, Microsoft 365 Groups (SharePoint site and mailbox), other SharePoint sites and OneDrive. They cannot be applied to Teams chats or posts.

## What is the difference between Data Lifecycle Management and Records Management

The main difference between these two options is licensing and functionality.

- Users with E3 or E5 licences that are assigned to roles giving access to the Data Lifecycle Management section of Purview can create and implement both retention policies and retention labels. Users with E3 licences can only create retention labels that will be 'manually' applied (e.g., auto-apply isn't allowed).
- End-users with E3 licences can 'manually' select and apply retention labels to individual items stored in Outlook, SharePoint and OneDrive. They can also (a) 'soft-delete' items that are subject to either a retention policy or label<sup>52</sup>, and (b) remove or change retention labels applied to these items.
- Users with E5 licences that are assigned to roles giving access to the Records Management section of Purview can create and implement file plan-based retention labels that include some additional functionality (see below) and set these to be auto-applied.

<sup>52</sup> Soft-deleted items are preserved in a hidden folder in Exchange Online mailboxes. In SharePoint and OneDrive, they are stored in the Preservation Hold library that can only be accessed by Site Collection Administrators.

- End-users with E5 licences can do everything an E3 licenced user can do (second dot point above), and can use the additional functionality such as the ability to (a) link them with terms from a Business Classification Scheme or File Plan, (b) auto-apply them, (c) associate them with a pre-defined event, and (d) link them with the disposition review functionality.

### Which one should you use?

Start with retention policies. But first, gain a detailed understanding of how both retention policies and labels work first, then plan the retention approach carefully with a full understanding of how these will work.

Understand the principles of retention, or ‘what takes precedence’, in Microsoft 365.<sup>53</sup>



*Image: Microsoft image showing the ‘principles of retention’*

Use retention labels selectively as ‘exceptions’ to, or to extend the periods set in, retention policies.

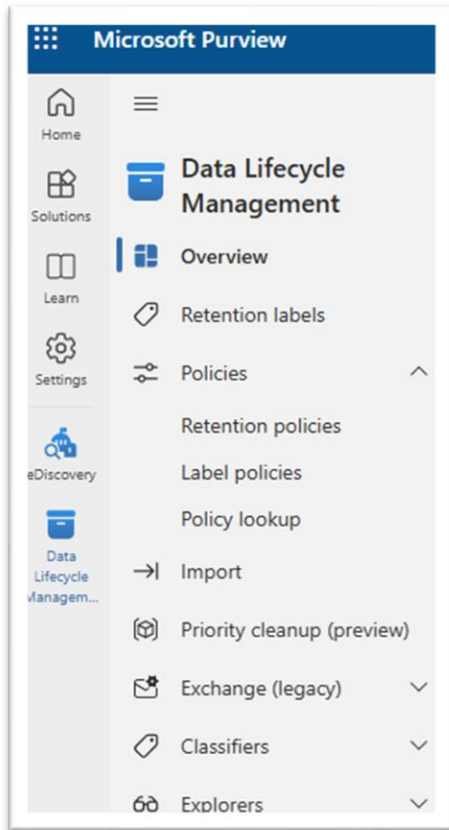
Both retention policies and retention labels are described in more detail below.

## Data Lifecycle Management

The Data lifecycle management section of Purview includes several options as shown in the image below. From a recordkeeping point of view, the key options are listed below. These are the subject of separate sections below:

- Policies – Retention policies
- Policies – Label policies
- Retention labels

<sup>53</sup> See: [Learn about retention policies & labels to retain or delete | Microsoft Learn](#), and [Principles of Retention in Microsoft 365 - Joanne C Klein \(accessed 5 May 2025\)](#)



*Image: Data Lifecycle Management options in Purview (May 2025)*

## Retention policies

**Note:** Retention policies described in this document are not intended to be used to implement retention periods as retention policies are too broad and do not ‘tag’ individual or logical aggregations of items.

Retention policies should only be used to prevent the unauthorised deletion of State records and hold records in place prior to formal appraisal and disposal activities.

Retention policies created in Purview create a back-end system process, a type of retention ‘hold’ that prevents the permanent deletion of individual items by capturing anything that is ‘soft-deleted’ in a secure location for the defined retention period. What happens at the conclusion of the retention period depends on how the policy is configured.

Retention policies:

- May be applied to all or selected Exchange mailboxes, Microsoft 365 Groups (SharePoint site and Exchange mailbox), non-Group-based SharePoint sites, Teams chats, Teams standard and shared channel posts, Teams private channel posts, Viva Engage (formerly Yammer) content, Copilot engagements and Enterprise AI Apps messages.
- Define a retention period (e.g., 10 years) based on one of (only) two triggers - ‘date created’ or ‘date modified’.

- Define what happens at the conclusion of the retention period for each item in the workload where they have been applied. The options are: (a) Delete items automatically (NOT recommended for content stored in Exchange mailboxes, SharePoint or OneDrive), or (b) Do nothing (recommended – see below). The third option to ‘Retain items forever’ should not be selected as it results in open-ended retention.

### **The meaning of ‘Do nothing’ at the end of the retention period**

Individual items that were ‘soft-deleted’ while the retention policy still applies will be stored in a hidden location and remain discoverable. End users will usually be unaware that these items are being ‘preserved’ in this way. These soft-deleted individual items will be automatically deleted by the system at the conclusion of the retention period that applies to them.

- For example, if an end user deletes an item in a mailbox, OneDrive or SharePoint site that is subject to a 10-year retention period, the item will be automatically deleted 10 years after it was created or modified regardless of whether the mailbox, OneDrive or SharePoint site remains active.

At the end of the retention period, the retention ‘hold’ will no longer apply to individual items.

- Items that are or were already deleted by end users in active mailboxes, Teams, SharePoint sites and OneDrive will be deleted permanently (instead of being preserved) because the items are no longer subject to a retention ‘hold’. Public offices need to be aware of this possibility and establish a process to ensure that any records in these workloads that need to be retained for longer: (a) are not destroyed - by applying a new retention policy or label, (b) removing all ‘delete’ permissions, or (c) moving them to a different location.
- Items that are stored in active or inactive SharePoint sites will need to be appraised for disposal action, or further retention applied if they need to be retained for longer. Public offices will need to establish a process to identify and manage the items in these sites that become due for appraisal and disposal action or further retention. If the site remains active, only specific items may be subject to appraisal and disposal actions. If the items are the only items in the site, the entire site may also be destroyed as part of the appraisal and disposal process. In this case, the destruction of the records AND the site should be recorded.
- Individual items in the Exchange mailbox and OneDrive of departed (deactivated) users, that were not deleted by end users before they departed (see below), will remain in those locations until the last items in either workload ceases to be subject to the retention ‘hold’. After that point, the entire mailbox or OneDrive will be automatically deleted by the system. Public offices that want to retain mailboxes as PST files, or retain the content stored in a OneDrive, should do this via Purview’s eDiscovery functionality.

### **Where can retention policies be applied?**

The screenshots below show the locations where retention policies can be applied. Each policy allows for specific users or locations to be included or excluded.

While one policy can be created for the first four (mailboxes, SharePoint classic and communication sites, OneDrives and Microsoft 365 Groups), it is better practice to create a single retention policy for each location because (a) there may be different retention

requirements for each, and (b) it is easier to disable a single policy for a single workload if required.

- Unless public offices have a requirement to do so, no retention policy is suggested for Skype for Business, Exchange public folders, or the two Yammer options (now Viva Engage).

Status	Location	Applicable Content	Included	Excluded
<input type="checkbox"/> Off	Exchange mailboxes	Items in user, shared, and resource mailboxes: emails, calendar items with an end date, notes, and tasks with an end date. Doesn't apply to items in Microsoft 365 Group mailboxes. <a href="#">More details</a>		
<input type="checkbox"/> Off	SharePoint classic and communication sites	Files in classic sites or communication sites or team sites that aren't connected to a Microsoft 365 group, and files in all document libraries (including default ones like Site Assets). <a href="#">More details</a>		
<input type="checkbox"/> Off	OneDrive accounts	All files in users' OneDrive accounts. <a href="#">More details</a>		
<input type="checkbox"/> Off	Microsoft 365 Group mailboxes & sites	Items in the Microsoft 365 Group mailbox, and files in the corresponding group-connected SharePoint team site. Doesn't apply to files in SharePoint classic or communication sites or SharePoint team sites that aren't connected to Microsoft 365 Groups. <a href="#">More details</a>		

<input type="checkbox"/> Off	Skype for Business	Skype conversations for the users you choose.		
<input type="checkbox"/> Off	Exchange public folders	Items from all Exchange public folders in your organization.		
<input type="checkbox"/> Off	Teams channel messages	Messages from channel conversations and channel meetings. Doesn't apply to Teams private channel messages. <a href="#">More details</a>		
<input type="checkbox"/> Off	Teams chats and Copilot interactions	Messages from individual chats, group chats, meeting chats, bot chats, and interactions with Microsoft Copilot for Microsoft 365. <a href="#">More details</a>		
<input type="checkbox"/> Off	Teams private channel messages	Messages from Teams private channels. <a href="#">More details</a>		
<input type="checkbox"/> Off	Yammer community messages	Messages from Yammer community discussions. <a href="#">More details</a>		
<input type="checkbox"/> Off	Yammer user messages	Private messages and community message notifications. <a href="#">More details</a>		

*Image: The various locations where retention policies may be applied in Purview. Note that 'Teams chats and Copilot interactions' can now be created as two separate policies. The image above shows the 'legacy' option visible in tenants as at 2 May 2025. See below for more information.*

See Attachment A for the recommended retention policies and details on how to separate Teams chats and Copilot interactions.

## Retention labels

As noted above, retention labels are created in two locations in Microsoft Purview.

- In the Data Lifecycle Management section of Purview (E3 and E5 licences).

- In the Records Management section of Purview (E5 licences).

### When to use labels

Retention labels cannot be applied to Teams chats or channel posts, Viva Engage posts, Copilot engagements or Enterprise AI apps messages.

Labels may be created as exceptions to extend the retention period of retention policies that have already been applied to a SharePoint site or Exchange mailbox.<sup>54</sup>

- For example, a Microsoft 365 Group (including its SharePoint site) may be subject to a 'back-end' 10-year retention policy with a 'Do nothing' action. This means that it would be possible to permanently delete items after that retention period has expired. To prevent this, retention labels may be used as exceptions to extend the retention period for specific records in the same site, thereby extending their retention beyond the 10-year retention policy period.

### Applying labels to folders in SharePoint (including Team-linked channel folders)

Although labels can be 'applied' to folders in SharePoint document libraries, the label itself is linked with the individual items stored in that folder, not the folder itself. This means that the system process that manages labels to determine if they can be deleted or other actions does not 'see' the folders.

- Public offices that have allowed the grouping of records in folders in document libraries could, from time to time, move ('archive') the content in older folders to new dedicated, read-only libraries where a retention label could then be applied to all the content. For example, a library that has folders grouping content by year.

### Applying labels to all items stored in libraries in SharePoint

A better approach with labels is to apply them to all items stored in libraries via the library setting 'Apply label to items in this library'. This is because libraries are a more logical way to aggregate records.

- For example, a SharePoint site may exist for many years, with all items covered by a 'back end' 10-year retention policy. A library on that site that was used to aggregate related records that map to a single retention class has become inactive. To ensure that all the records in that library are retained for the same period of time, a single retention label (mapped to a GA class) with the trigger of 'when the label was applied' (see below) could be applied to all items in the library. This means that all items in the library will become due for disposal at the same time in the future, thereby facilitating the eventual disposal of those records. Removing all edit permissions on the library will further help to protect the records from being soft-deleted or changed.

### Creating labels – recommended settings

The following are the recommended settings for all labels. Retention labels should always be based on individual classes in an approved RDA.

---

<sup>54</sup> See: [Create retention labels for exceptions | Microsoft Learn](#) (accessed 2 May 2025)

Option	Recommended setting
<b>Name</b>	<ul style="list-style-type: none"> <li>• Include enough information in the label name so that end users know what the label is and what it does. For example: 'GA28 7.1.1 Financial Management – Accounting – Financial Transactions – 7 years – Do nothing'</li> </ul>
<b>Description for users</b>	<ul style="list-style-type: none"> <li>• Use the same text as the retention class wherever possible. For example, 'Records documenting the organisation's financial transactions. Includes revenue, expenditure, debt recovery and deposits.'</li> </ul>
<b>Description for admins</b>	<ul style="list-style-type: none"> <li>• Provide a brief description of what the label will do</li> </ul>
<b>(E5 only, optional)</b> <b>Define file plan descriptors for this label</b>	<ul style="list-style-type: none"> <li>• This section may be used to add a reference ID, function, activity, authority type, and provision/citation. Note that these terms are not connected with any BCS taxonomy created in the SharePoint Term Store and will not be visible to the end user who applies the label.</li> </ul>
<b>(E3, E5)</b> <b>Define label settings</b>	<ul style="list-style-type: none"> <li>• Select 'Retain items forever or for a specific period'.</li> <li>• (E5 only) Select 'Enforce actions after a specific period'. This option provides for two outcomes (see below): (a) Delete items automatically (NOT recommended) or (b) Change the label. (Note: It may be useful to create a retention label with the name 'Ready for disposal' with no other options set ('Just tag items'). When the first label reaches the end of the retention period, the label would then be automatically changed to 'Ready for disposal' allowing the public office to locate records that are due for disposal. This action will facilitate appraisal and disposal actions.)</li> </ul>
<b>(E3, E5)</b> <b>Define the retention period</b>	<ul style="list-style-type: none"> <li>• Retain items for: The period indicated in the GA class (e.g., 7 years).</li> <li>• Start the retention period based on one of the following: (a) 'When items were last modified' (best for content in SharePoint and OneDrive), (b) 'When items were created' (best for content in mailboxes) OR (c) 'When items were labelled' (good option for SharePoint). Option (c) provides a way to ensure that all records in an aggregation become due for disposal at the same time and is generally recommend for this reason.</li> </ul> <p><i>Note:</i> Avoid using 'event type' triggers unless a risk-based decision has been made that these will always be accurate or the required 'Compliance Asset Id' has been accurately applied by end users.</p>

(E5 only)

Choose what happens during the retention period

- If 'Retain items forever or for a specific period' has been selected in the label settings, select 'Retain items even if users delete'.
- (Optional) The option to 'Mark items as a record' provides a way to items being deleted from the library, or the label removed. See note below

(E3, E5)

Choose what happens after the retention period

- (E3) Select 'Deactivate retention settings' (= Do nothing)
- OR
- (E3) Select 'Change the label'. This option presents the option to 'Choose a replacement label', for example a label that just tags items with the name 'Ready for disposal'.
- (E3) Do not select any of the other options.
- (E5) If 'Retain items forever or for a specific period' has been selected in the label settings above, select either 'Change the label' OR 'Deactivate retention settings'.
- OR
- (E5) If 'Enforce actions after a specific period' has been selected in the label settings, select 'Change the label'. This option presents the option to 'Choose a replacement label'. Do NOT select 'Delete items automatically'.

*Note:* The options 'Delete items automatically' (E3, E5), 'Start a disposition review' (E5 only), or 'Run a Power Automate Flow' (E5 only) are not recommended unless there is a specific business case for using these options and, for the auto-delete option, there has been an assessment of the risks associated with auto-deletion.

---

## Marking items as a record

The option to 'mark items as a record' is based on requirement in the United States standard DoD 5015.02-STD<sup>55</sup> that an 'information product' is not a record unless or until it is 'declared' as one.

This does not apply in NSW. A record does not need to be marked as a record to be a record. Under the State Records Act a record is defined as any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means, and a State record is a record made or received in the course of exercising official functions in a public office, or for a purpose of a public office, or for the use of a public office.

However, for the purposes of M365, State Records NSW notes : 'Content needs to be declared as a record to be defined as a record in M365. Without the record declaration, metadata, retention and/or disposal documentation will not be retained. This will need to be configured in M365 settings.'<sup>56</sup>

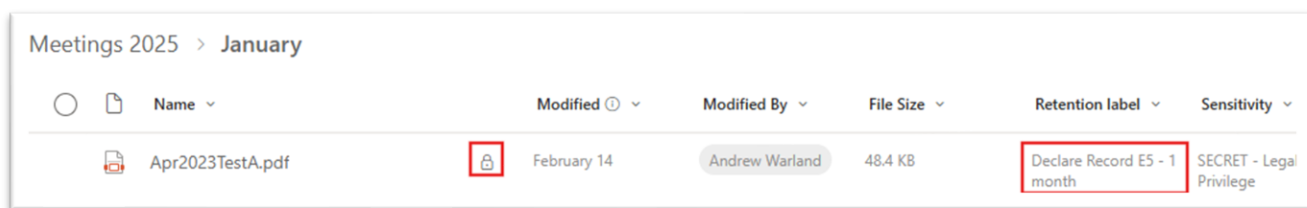
An E5 licence is required to use this additional functionality in Microsoft 365. When the label is configured, the option appears to 'declare as record' when the label is applied.

---

<sup>55</sup> See: [DoD 5015.02-STD Electronic Records Management Software Applications Design Criteria](#) (accessed 2 May 2025)

<sup>56</sup> Source: [Microsoft 365 and recordkeeping | NSW Government](#) (accessed 5 May 2025)

When labels with this option are applied, a small padlock icon appears next to the records that have been labelled in the library.

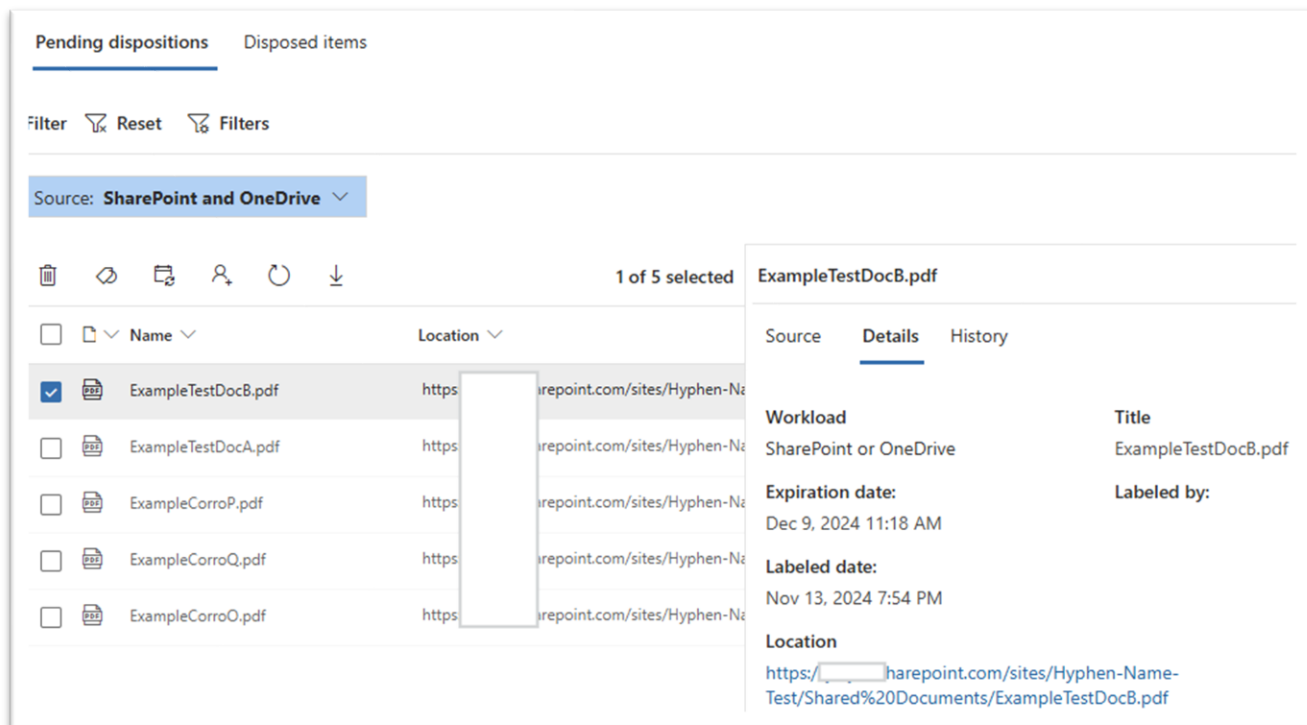


**Image:** The small padlock that appears next to an item when the 'Declare Record' option is used with a label. Note that the retention label can have any name, the naming shown in the image is for demonstration purposes only.

### Disposition (not recommended)

The 'Disposition' feature available in the Records Management section of Purview for public offices with E5 licences is not recommended for the following reasons:

- It presents individual items for review, out of context of any other records from the same location.
- Insufficient metadata is presented with each record (see image below).
- Insufficient information is captured about who approved the disposal, and it is not exportable.
- Insufficient metadata is retained about records that have been destroyed, and this information is not held forever.



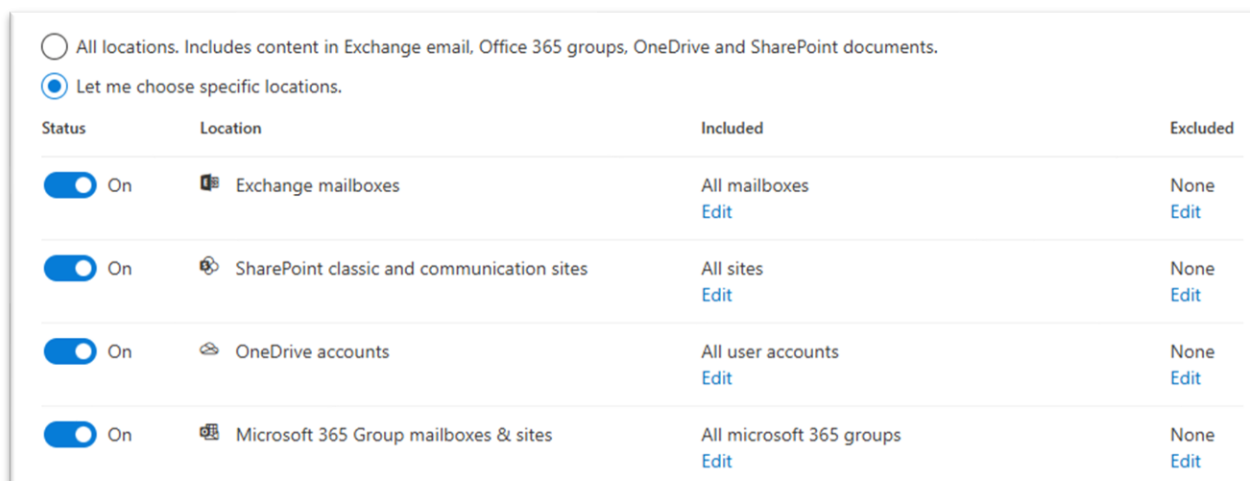
**Image:** How individual items appear in the 'Pending dispositions' area of Dispositions.

A better option 'out of the box' is to establish a process to export the full set of metadata (in a view) of records in SharePoint libraries that are due for disposal, then use this exported file to request approval for disposal. A record of the original metadata and

approval should then be stored in a separate, dedicated location, and the records subject to the approval can be destroyed. If the records are the only content in the library, the library can also be destroyed. If the library is the only one in the site, the site can also be destroyed. The destruction of libraries and sites should also be recorded.

## Publishing labels

Retention labels do not do anything until they are published in a label policy. It is the label policy that makes labels visible in the locations where they will be used.



*Image: Locations where labels may be published to.*

While labels can be published at once to all workload locations (as shown in the image above), it is more useful and practical to publish select labels to the specific locations where they are most likely to be used. Otherwise, end users might have to select from a very long list of labels on every site.

- For example, publish labels mapped to classes under the GA28 function of 'Financial Management' only to SharePoint sites that are known to contain financial records.

The recommended options for label policies are as follows:

Option	Recommended setting
Select the labels to be included in this policy	<ul style="list-style-type: none"> <li>• (Selected labels)</li> </ul>
Choose the type of retention policy to create	<ul style="list-style-type: none"> <li>• Static (E3 and E5 licences)</li> <li>• Adaptive (E5 licences)</li> </ul>
Publish to users and groups	<ul style="list-style-type: none"> <li>• Select the relevant mailboxes, sites, OneDrive accounts, or Microsoft 365 Groups rather than default unless a label is likely to be required in every location.</li> <li>• Note: There may be a requirement for some labels to be available in every location. This outcome can be achieved</li> </ul>

by creating a separate label policy rather than adding it to every label policy.

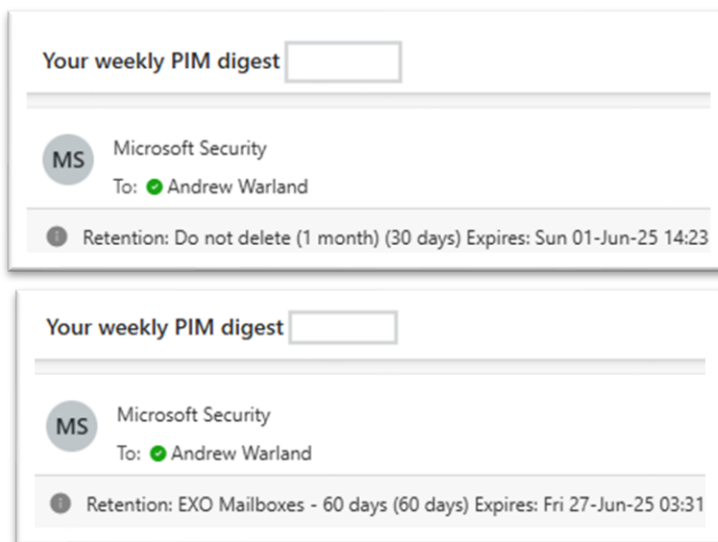
**Name of policy**

- The name should clearly indicate what type of labels are included. For example, 'Financial management records'. Note that the name of the label policy will not be visible to any end users.
- Provide a description so that users will know what it is used for and its intended scope. For example, 'This policy includes finance-specific labels mapped to relevant classes in GA28 and is only applicable to sites with financial records covered by the label'.

**After publishing labels**

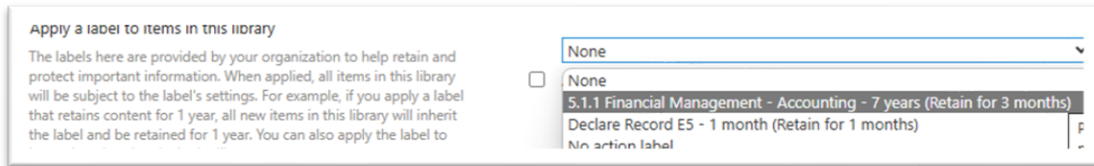
Once published, labels may be applied in several ways.

- In **Outlook**, a label may be applied directly to an email or folder via the 'Policy' setting. Be aware that MRM tags may also still appear via this method – refer to the section about MRM for more information. If a retention policy has been already applied, the name of that retention policy will be shown as can be seen in the first image below ('Retention: EXO mailboxes – 60 days'). When a label is applied, this will be replaced by the name of the retention label ('Retention: Do not delete (1 month)') as can be seen in the second image). If no retention details appear, this is probably because the default MRM policy has been applied. See section 7.7 below.



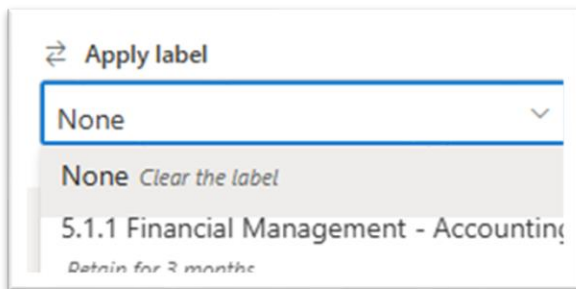
*Images: How a change to retention appears in an email in Outlook*

- In a **SharePoint site library**, a label may be applied to a library via Library Settings – More library settings, 'Apply label to items in this list or library' as shown in the image below. Choose the label from the drop-down list. (If no labels appear, then the label may not have been correctly published, or you may need to wait a few hours). The option to 'Apply label to existing items in this library' may be used to apply the label to all items. This option is particularly useful if there is a need to close the library from further edits (e.g., make it read only) and apply a label that has the trigger option 'When the label was applied'.



*Image: Application of a retention label to a library. The label starting with '5.1.1' relates to a different jurisdiction and is an example only.*

- For items stored in a **SharePoint site library**, a label may be applied by selecting a specific folder or document and, from the information panel on the top right, choosing the required retention label from the drop-down list under 'Apply label'. This will apply the label to all items in the folder, or to the document/s that was selected.



*Image: Applying a retention label via the 'details' panel*

**Notes:**

- When retention labels are applied by end users or automatically to individual items in a library, end users with edit rights can remove or change these labels via the 'Details' panel, as shown in the image above.
- While a retention label may be applied to a folder, and all items 'in' the folder will be tagged with the label, the label does not technically apply to the folder. This means that folder-based libraries with the disposal action of 'Destroy automatically' will eventually end up with a series of empty folders with no items stored 'in' them.

**Auto-applying labels**

Organisations with E5 licences might consider using the auto-apply option to apply labels to content in their Microsoft 365 environment. This outcome is achieved by creating an auto-labelling policy. Organisations who choose this option should exercise care to ensure that any auto-applied labels will accurately and consistently apply the label to the correct items.

The following elements are required for an auto-label policy:

Setting	Option
<b>Name and description</b>	<ul style="list-style-type: none"> <li>• Provide a name to indicate what the policy does</li> </ul>
<b>Choose the type of content that you want to apply this label to</b>	<ul style="list-style-type: none"> <li>• Apply label to content that contains sensitive information</li> <li>• Apply label to content that contains specific words or phrases, or properties</li> <li>• Apply label to content that matches a trainable classifier</li> </ul>

	<ul style="list-style-type: none"> <li>• Apply label to cloud attachments and links shared in Exchange, Teams, Viva Engage and Copilot</li> </ul>
<b>Policy scope</b>	<ul style="list-style-type: none"> <li>• Select any Admin Units that may use this policy.</li> </ul>
<b>Type of retention policy</b>	<ul style="list-style-type: none"> <li>• Adaptive</li> <li>• Static</li> </ul>
<b>Choose adaptive policy scopes and locations</b>	<ul style="list-style-type: none"> <li>• Select the adaptive policy scope and locations</li> </ul>
<b>Choose the label</b>	<ul style="list-style-type: none"> <li>• Select the label to be included in the policy</li> </ul>
<b>Mode</b>	<ul style="list-style-type: none"> <li>• Test the policy before running it</li> <li>• Turn on policy</li> </ul>

## Alternatives to retention policies or labels

Within the last ten years, Microsoft have changed the way retention works several times. Additionally, retention policies and labels are not 'transferrable' to another tenant, which is particularly relevant for public offices that may be subject to Machinery of Government changes.

There are two primary alternatives to the use of retention policies or retention labels.

### Alternative to retention labels in SharePoint

Instead of creating and deploying multiple GA-class-mapped retention labels, public offices could do the following, for at least some SharePoint libraries.

- Create a taxonomy in the Managed Metadata Service (Term Store) using the Function, Activity and Class number and name (abbreviated as required).
- Create or use a single retention label 'Do not destroy' using the 'Retain forever' option. This will prevent items being destroyed permanently. The E5 capability to 'Declare a record' will 'lock' the record and prevent changes or deletions.

In SharePoint, the terms from the Managed Metadata Service can be applied to individual items (not folders) via site columns added to each library, along with the single retention label.

The end result is that each item in the library will have the following metadata:

- Function (e.g., 'Financial Management')
- Activity (e.g., 'Accounting')
- Class (e.g., '7.1.1 Financial Transactions – 7 years')
- Retention label (e.g., 'Do not destroy')

The 'Modified' date in the library will show when items were last modified which, in many cases, will be the suitable alternative to the 'date of last action'.

When ready for disposal, a view can be created filtered by the items with the relevant class. The full set of metadata in the view can then be exported for disposal review and approval.

This method may be useful for public offices that need to transfer records to a different public office.

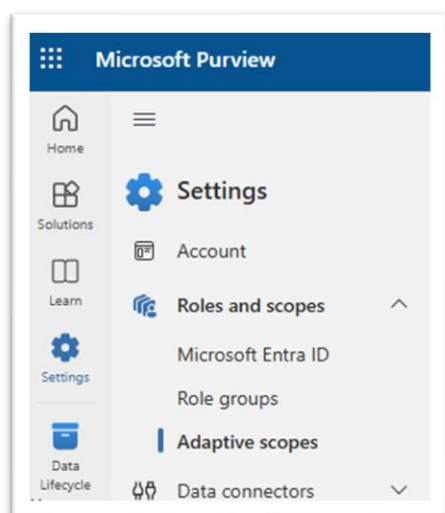
### Alternative to retention policies or labels for long-term public office retention in SharePoint

For records that need to be retained by public offices for more than ten years, such as records documenting the appointment and subsequent employment history of employees (GA28, class 15.4.3), public offices could apply a short-term (e.g., 7 years) retention policy that prevents the permanent destruction of records for a given minimum period and, once the employee has left the organisation, remove all edit rights on their 'file'.

- Note that document sets, not folders, are more suitable for this option because folders can contain multiple additional folders.

## Adaptive scopes

The option to select an adaptive scope appears in both retention policies and retention labels.



*Image: Location of 'Adaptive scopes' option in Purview*

Adaptive scopes '... use a query that you specify, so you can define the membership of users or groups included in that query. These dynamic queries run daily against the attributes or properties that you specify for the selected scope. You can use one or more adaptive scopes with a single policy'<sup>57</sup>

There are three types of adaptive scope as indicated in the image below – Users, SharePoint sites, and Microsoft 365 Groups.

<sup>57</sup> Source: [Adaptive scopes | Microsoft Learn](#) (accessed 2 May 2025)

## What type of scope do you want to create?

Each type of scope uses different attributes or properties to match the users, sites, or groups you want to detect in a policy.

- Users**  
You'll select Microsoft Entra ID attributes used to define users (such as First name, Last name, and Department).
- SharePoint sites**  
You'll select SharePoint properties used to define sites (such as site name, site URL, and refinable strings).
- Microsoft 365 Groups**  
You'll select Microsoft Entra ID attributes used to define groups (such as Name, Description, and Email address).

*Image: Adaptive scope options*

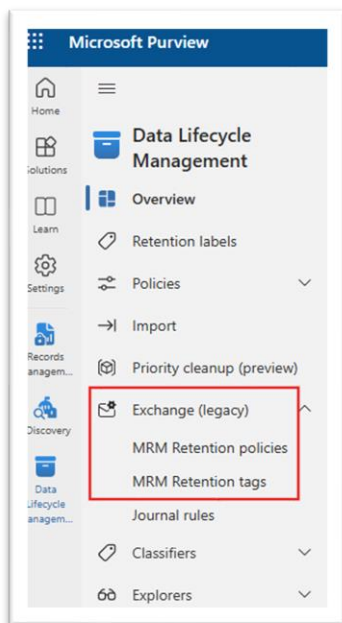
There are several advantages of using adaptive scopes, including no limits on the number of items per policy, more powerful targeting of policies, resilience against business changes and support for Microsoft Entra administrative units.<sup>58</sup>

Public offices with E5 licences should consider the use of adaptive scopes in their planning for retention.

## Legacy Exchange Online Messaging Records Management

Exchange Online mailboxes still include the legacy option to apply a Messaging Records Management (MRM) policy to mailboxes, and this option frequently remains deployed in many public offices.

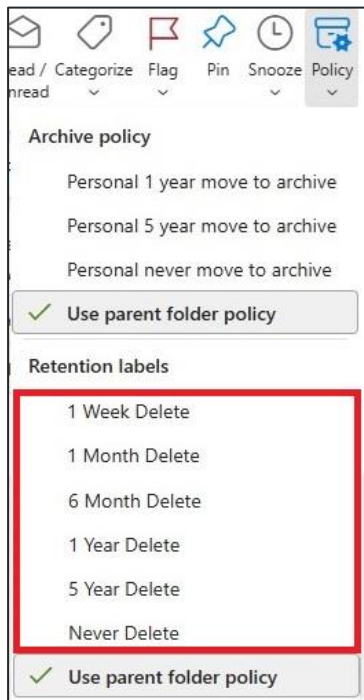
MRM retention options are now tagged as being 'Legacy' options as can be seen in the image below.



*Image: Exchange (legacy) options in Purview*

<sup>58</sup> Ibid

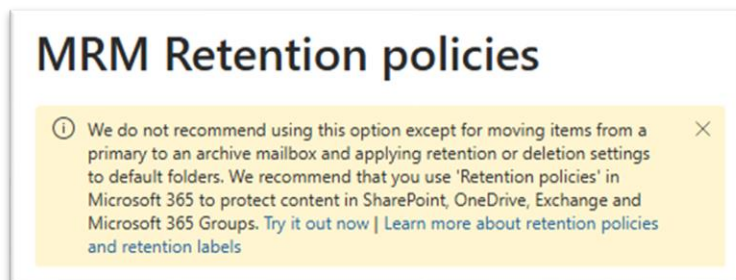
MRM tags can be seen when an email is selected via the 'Policy' option in Outlook, as shown in the image below. MRM 'Delete' tags are highlighted.



*Image: Default archive policies (top) and delete tags (in the red box) that are visible in Outlook*

As can be seen in the image above, the default MRM policy includes several 'Delete' tags that would allow end users to tag items to automatically delete them after a given period (if no other retention has been applied) or never delete them.

These tags are now described by Microsoft as a legacy functionality, as indicated in the image below.



*Image: Notification in the MRM section of Purview about the use of MRM retention policies*

Public offices should:

- Remove all the 'Delete' tags in the MRM policy and instead use Microsoft 365 retention policies or retention labels as described in this document.
- Leave the 'Archive' tags in place as these can be used in combination with online archiving capabilities in mailboxes.

## Information sensitivity labels

Information sensitivity labels are created in the Information Protection section of Microsoft Purview. Sensitivity labels should be created in line with NSW Government requirements for information classification, labelling and handling.<sup>59</sup>



Image: NSW security classifications

The table below describes the recommended settings for sensitivity labels created in Purview to align with NSW security classifications.

Label name (priority should be from 0)	Recommended scope	Recommended settings	Included Groups and sites?
UNOFFICIAL (priority 0)	Items – Files, Emails	Apply content marking: (Header and Footer, 14 point, red, centred)  Control access - UNCHECKED  No auto-labelling	No
OFFICIAL	Items – Files, Emails	Apply content marking: (Header and Footer, 14 point, red, centred)  Control access - UNCHECKED  No auto-labelling	No

<sup>59</sup> See: NSW Government Information Classification, Labelling and Handling Guidelines | Data.NSW (accessed 5 May 2025)

<b>OFFICIAL: Sensitive – (plus relevant Dissemination Limiting Marker)</b>	Items – Files, Emails	Apply content marking: (Header and Footer, 14 point, red, centred)  Control access - UNCHECKED  No auto-labelling	No
<b>PROTECTED</b>	Items – Files, Emails  Groups & Sites	Apply content marking: (Header and Footer, 14 point, red, centred)  Control access/Access control:  <ul style="list-style-type: none"> <li>• Configure access control settings – Let users assign permissions when they apply the label.</li> <li>• In Outlook – SELECT Encrypt only</li> <li>• In Word, PowerPoint and Excel, UNCHECK prompt user to specify permissions</li> <li>• (Do not check ‘Use Double Key Encryption’)</li> </ul> No auto-labelling	Groups and sites:  Privacy and external user access – UNCHECKED  External sharing and Conditional Access – CHECKED.  (a) Control external sharing from label SharePoint sites UNCHECKED.  (b) User Microsoft Entra Conditional Access to protect labelled SharePoint sites – CHECKED IF REQUIRED (and note additional requirement in SharePoint)  Private teams discoverability and shared channel settings - UNCHECKED  Apply a label to channel meetings - UNCHECKED
<b>SECRET</b>	Items – Files, Emails  Groups & Sites	Apply content marking: (Header and Footer, 14 point, red, centred)  Control access/Access control:  <ul style="list-style-type: none"> <li>• Configure access control settings – Let users assign permissions when they apply the label.</li> </ul>	Groups and sites:  Privacy and external user access – UNCHECKED  External sharing and Conditional Access – CHECKED.

	<ul style="list-style-type: none"> <li>In Outlook – SELECT Encrypt only</li> <li>In Word, PowerPoint and Excel, UNCHECK prompt user to specify permissions</li> <li>(Do not check ‘Use Double Key Encryption’)</li> </ul>	<p>(a) Control external sharing from label SharePoint sites UNCHECKED.</p> <p>(b) User Microsoft Entra Conditional Access to protect labelled SharePoint sites – CHECKED IF REQUIRED (and note additional requirement in SharePoint)</p>
	No auto-labelling	Private teams discoverability and shared channel settings - UNCHECKED
		Apply a label to channel meetings - UNCHECKED

### Sensitivity labels linked with SharePoint permissions

In early 2025, Microsoft introduced a new option to ‘Configure SharePoint with a sensitivity label to extend permissions to downloaded documents.’<sup>60</sup> This option links sensitivity labels with permission set in SharePoint sites but only applies to Office documents and PDFs stored in a library (e.g., not to images and other formats). If the item subject to one of these labels is downloaded, moved or copied, it can only be accessed by whoever has access in the SharePoint library – including when changed at any time.

The table below shows the recommended settings for this type of label.

Label name (priority should be from 0)	Recommended scope	Recommended settings	Included Groups and sites?
<b>Example: ‘SECRET – ACCESS CONTROLLED’</b>	Items – Files (No other option is possible)	Apply content marking: (Header and Footer, 14 point, red, centred)  Control access/Access control: <ul style="list-style-type: none"> <li>Configure access control settings – Let users assign permissions when they apply the label.</li> </ul>	No

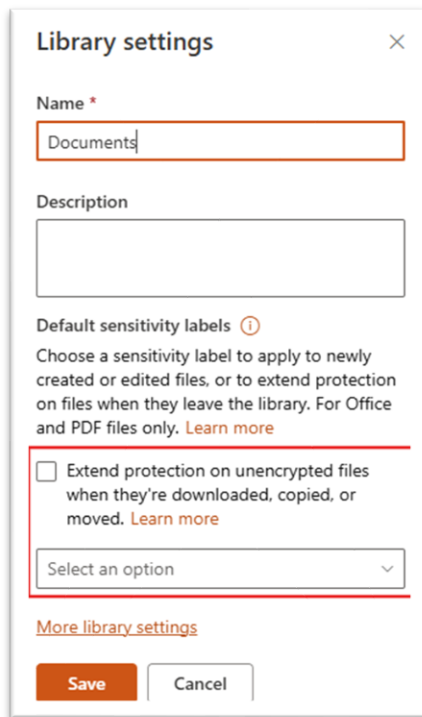
<sup>60</sup> For more information, see: [Configure SharePoint with a sensitivity label to extend permissions to downloaded documents | Microsoft Learn](#) (accessed 2 May 2025)

- In Word, PowerPoint and Excel, UNCHECK prompt user to specify permissions

DO NOT check the Outlook option.

No auto-labelling

The image below shows how this option appears when implemented (in the red box). The ability to set a default sensitivity label remains for site owners but only users who have been included in the setting for the special label can check the option to 'extend protection' and select the special label instead. When a label is applied in this way, it will replace any default label and override all other sensitivity labels except labels that include encryption.



*Image: The option to apply a sensitivity label to extend SharePoint permission to unencrypted files in library settings.*

This option should only be used for specific types of sensitive content stored in certain SharePoint sites.

### Information Management Markers (IMMs)

NSW government guidelines states that there are six Dissemination Limited Markers (DLMs).

- NSW Cabinet
- Legal
- Law enforcement
- Health information

- Personal
- NSW Government

If any of these DLMs are required, a new label should be created with a hyphen between the original name and the DLM, e.g., 'PROTECTED-Legal Privilege', rather than being a sub-label. The same options as listed above should be used.

Additional settings may be used, for example to control access or linked with conditional access policies. These should be documented.

### Labels must be published

Sensitivity labels must be published before they will be available to end users.

When publishing a label, organisations should consider publishing each label separately, rather than all at once in a single sensitivity policy. This will assist with making changes as required to individual labels and policies.

The following are the recommended settings for these label policies.

Option	Settings
<b>Choose sensitivity labels to publish</b>	<ul style="list-style-type: none"> <li>• Select the labels to be published.</li> </ul>
<b>Admin units</b>	<ul style="list-style-type: none"> <li>• Accept the default 'Full directory' unless there is a requirement to restrict who can see the label.</li> </ul>
<b>Users and groups</b>	<ul style="list-style-type: none"> <li>• Accept the default 'All users &amp; groups' unless the label needs to be restricted to a particular set of users or groups. For example, a Security Group that includes a set of accounts that are allowed to use a specific label.</li> <li>• For the 'access controlled' special labels, select the names of only those users who will be allowed to use the label (e.g., check the box in the SharePoint library).</li> </ul>
<b>Settings</b>	<ul style="list-style-type: none"> <li>• Users must provide a justification to remove a label or lower its classification. CHECKED for any label PROTECTED and above (including DLMs).</li> <li>• Require users to apply a label to their emails and documents. CHECKED for any label PROTECTED and above (including DLMs).</li> <li>• Require users to apply a label to their Fabric and Power BI Content. UNCHECKED unless this is a requirement.</li> <li>• Provide users with a link to a custom help page. CHECKED if the organisation has created such links.</li> </ul>
<b>Default settings for documents, emails, meetings,</b>	<ul style="list-style-type: none"> <li>• Consider selecting the base level 'OFFICIAL' label for both documents and emails.</li> <li>• Inherit label from attachments. CHECK: (a) 'Email inherits highest priority label from attachments' and (b) 'Recommend</li> </ul>

<b>Fabric and Power BI</b>	<p>users apply the attachment's label instead of automatically applying it'.</p> <ul style="list-style-type: none"> <li>• Meetings: No default label, UNCHECK 'Require users to apply a label to their meetings and calendar events'.</li> <li>• Fabric and Power BI content. No default label.</li> </ul>
<b>Name</b>	<ul style="list-style-type: none"> <li>• Name of the policy.</li> </ul>

## Data Loss Prevention

Data Loss Prevention (DLP) in Microsoft 365 provides the ability, through pre-defined policies, to protect sensitive data, reduce the risk of oversharing, and prevent end-users from inappropriately sharing sensitive data with people who shouldn't have access to that data. DLP policies, created in Purview, allow an organisation to identify, monitor and automatically protect sensitive data.<sup>61</sup>

DLP policies use 'deep content analysis' based on the following:

- Keyword matching.
- Evaluation of regular expressions ('regex').
- Internal function validation.
- Matching with information sensitivity labels.
- Machine learning methods.

Public offices should implement DLP policies to protect sensitive data and records.

## Communication Compliance

Communication Compliance in Purview is an insider risk solution that allows organisations to detect regulatory compliance and business conduct violations such as misuse of sensitive or confidential information, harassing or threatening language, conflict of interest and sharing adult content.<sup>62</sup>

Public offices with a requirement to monitor communication compliance, especially in relation to the misuse of sensitive or confidential information, should consider making use of this section.

## Insider Risk Management

According to Microsoft, 'Insider Risk Management correlates various signals to identify potential malicious or inadvertent insider risks, such as IP theft, data leakage and security violations. Insider Risk Management enables customers to create policies to manage security and compliance. Built with privacy by design, users are pseudonymised by default, and role-based access controls and audit logs are in place to help ensure user-level privacy.'<sup>63</sup>

<sup>61</sup> **Source:** [Learn about data loss prevention | Microsoft Learn](#) (accessed 2 May 2025)

<sup>62</sup> **Source:** [Learn about communication compliance | Microsoft Learn](#) (accessed 2 May 2025)

<sup>63</sup> **Source:** [Learn about insider risk management | Microsoft Learn](#) (Accessed 2 May 2025)

Internal risks can include any of the following:

- Leaks of sensitive data and data spillage.
- Confidentiality violations.
- Intellectual property (IP) theft.
- Fraud.
- Insider trading.
- Regulatory compliance violations.

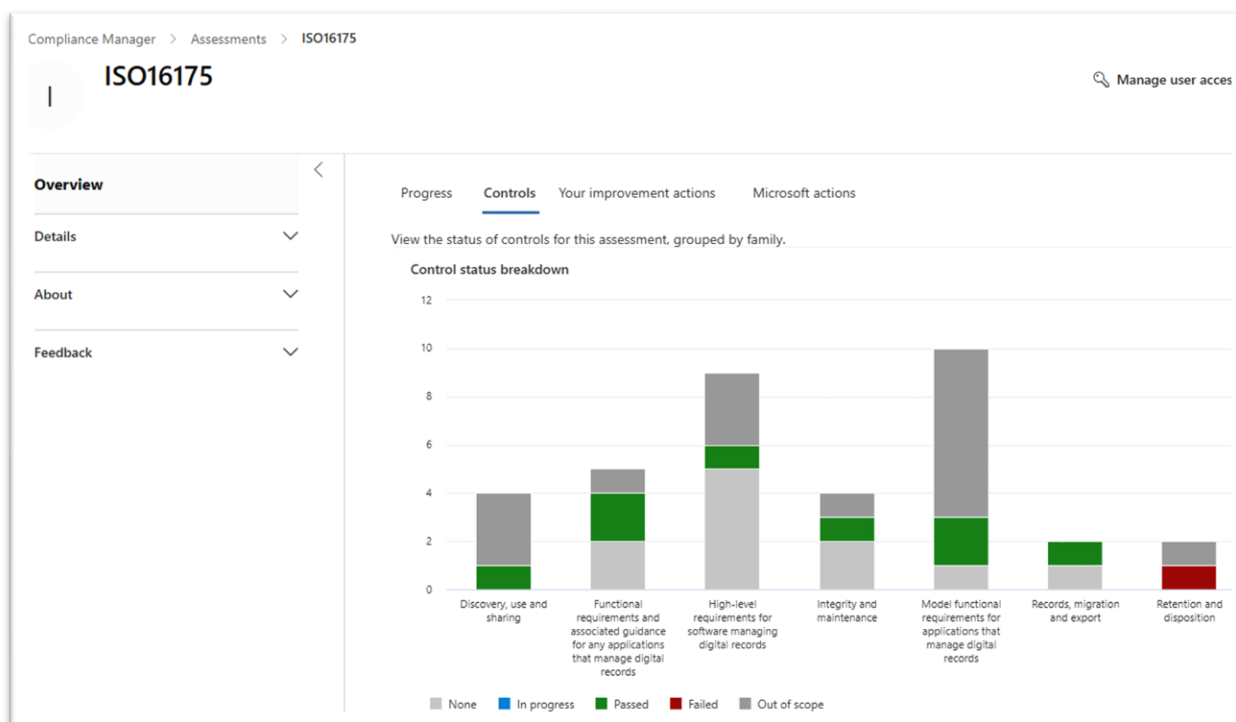
Public offices might consider using the Insider Risk Management functionality to identify and take action in relation to any of the above risks.

## Compliance Manager

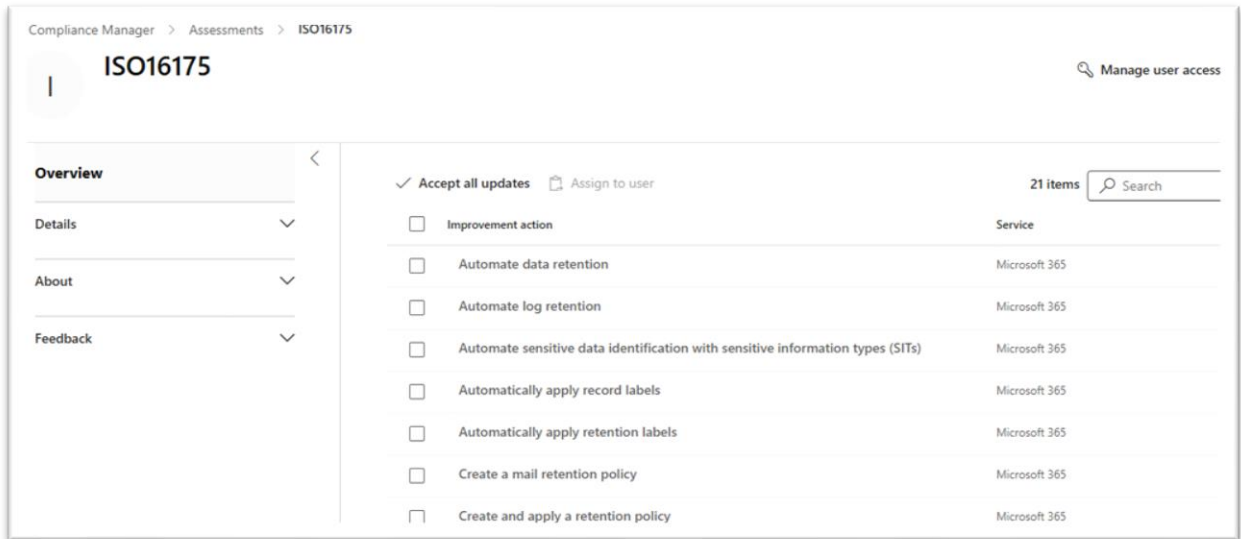
The Compliance Manager section of Purview allows public offices to ‘measure progress in completing actions that help reduce risks around data protection and regulatory standard’. An extensive range of standards are available, including ISO 16175.

The Compliance Manager tool reports on an organisation’s compliance with these standards and offer options for improvement.

The image below shows an example of the status of controls for an assessment against ISO 16175.



*Image: Example of the status of controls against ISO 16175*

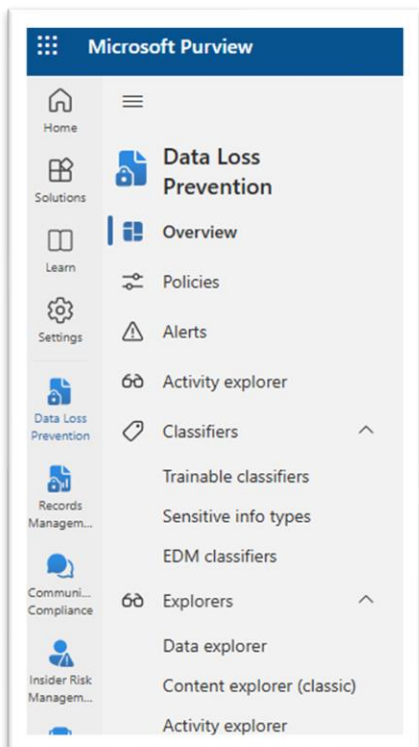


**Image:** The image above shows a list of suggested improvement actions for the tenant against ISO 16175. These actions, or a report, can be downloaded.

## AI and Machine Learning classifiers, Data explorers (E5)

AI and Machine Learning capabilities in Purview provide records and information managers (and organisations generally) that have an E5 licence with the ability to understand and manage content, including records, more effectively, by identifying where it is and then (optionally) applying additional controls to that content.

**Note:** Previously, the Artificial Intelligence (AI) and Machine Learning (ML) capabilities in Purview were in a separate 'Data Classification' section. The functionality is now available within the Purview sections described above, under the general heading of 'Classifiers' and/or 'Explorers' (not all sections have both options), as can be seen in image below.



**Image:** Classifiers and Explorers in Data Lifecycle Management

## Classifiers

Classifiers in Purview provide a mix of AI and ML capabilities that enable organisations to find and, if required, protect or manage that information. For example, a classifier might be used to identify Legal agreements stored across Microsoft 365 and then apply a retention or sensitivity label to that content.

The Classifiers section in Purview includes three options.

- Trainable classifiers. These classifiers use automated pattern-matching to identify content.
  - Microsoft provide over 100 trainable classifiers, designed to detect content that matches the trained items. For example, Agreements, Bank statement, Budget, Business Plan, Customer Complaints, HR, Health/Medical forms, Invoice, Legal Deeds, Legal Agreements, Procurement, Quotation, Regulatory Collusion and so on.<sup>64</sup>
  - Organisations may create their own trainable classifiers noting, as the name suggest, there is a requirement to ‘train’ the system to recognise matching samples. This can take time. See also the related section on Microsoft Syntex in Attach. B.
- Sensitive info types (SITs). Sensitive information types are designed to identify sensitive (or potentially sensitive) information, using Regular Expressions (‘regex’) and other known signals to identify such content. SITs only work with text-based (e.g., readable) content.<sup>65</sup>
- Exact Data Match (EDM) classifiers. According to Microsoft ‘Exact data match (EDM) classifiers use exact values from your org’s data to detect matches instead of generic patterns.’<sup>66</sup> No EDM classifiers are provided ‘out of the box’ in Purview, they must be created.

## Explorers

The Explorers section includes the new ‘Data explorer’, the legacy ‘Content explorer’ and ‘Activity explorer’.

### Data Explorer

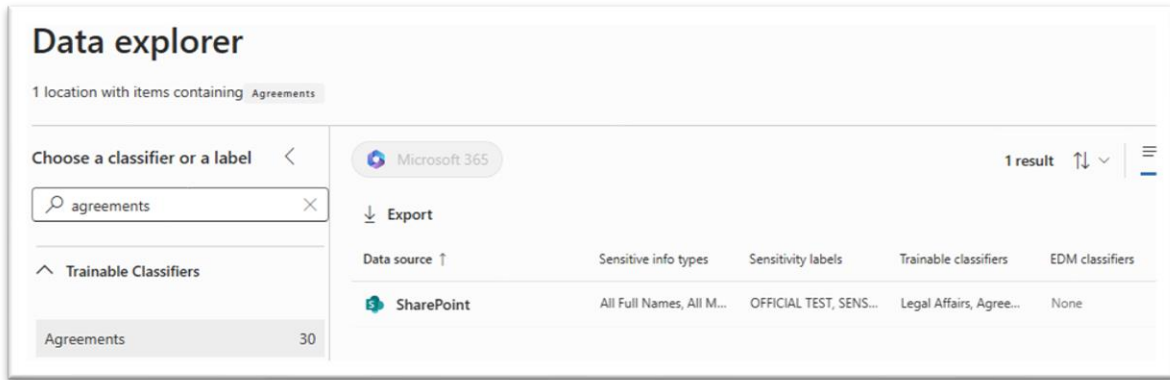
The Data Explorer option presents, for each classifier, as well as each sensitivity label and retention label (but not retention policy), where content that matches the classifier is (or may be) located. For example, in the image below, records in three locations show matches against pre-defined sensitive info types, sensitivity labels, trainable classifiers and retention labels.

---

<sup>64</sup> **Source:** [Learn about trainable classifiers | Microsoft Learn](#) (accessed 2 May 2025)

<sup>65</sup> **See** the Microsoft listing of Sensitive Info Types and what they are trained to find: [Sensitive information type entity definitions | Microsoft Learn](#) (accessed 2 May 2025)

<sup>66</sup> **Source:** [Learn about exact data match based sensitive information types | Microsoft Learn](#) (accessed 2 May 2025)



*Image: Example Data explorer view.*

It is possible to ‘drill down’ into any of the data sources shown by clicking on it as can be seen in the image below. Note the message in the yellow bar that the ‘actual number of items ... might be different from the calculated number that’s display on the left’. There is clearly a difference between the ‘30’ above and the ‘9’ below.



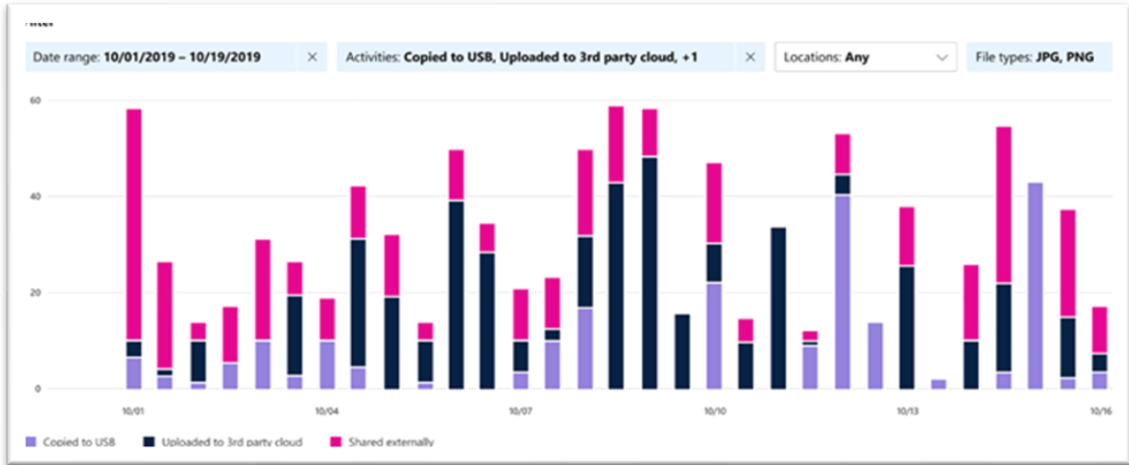
*Image: Example Data explorer view, after the primary data source is selected.*

The Data explorer function provides records managers with the ability to identify the location of records that may be stored in Exchange mailboxes, Teams, SharePoint and OneDrive. Generally, the ‘Trainable Classifiers’ is more accurate than the SITs area.

### Activity explorer

The Activity explorer option allows organisations to ‘review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and more. Label activity is monitored across Exchange, SharePoint, OneDrive, and endpoint devices’. The example image below comes from Microsoft.<sup>67</sup>

<sup>67</sup> Source: [Get started with Activity explorer | Microsoft Learn](#) (accessed 2 May 2025)



*Image: Example content from Activity explorer in Purview (Microsoft image)*

# Attachment A – Recommended retention policies

**Note:** Retention policies described in this document are not intended to be used to implement retention periods in line with RDA classes as retention policies are too broad and do not tag individual items.

Retention policies should be used to prevent the unauthorised deletion of State records and hold records in place prior to formal appraisal and disposal activities.

## Retention policy for personal and shared mailboxes

One retention policy is recommended for personal and shared mailboxes, noting that the mailboxes of select roles will be exported to PST after those individuals leave the organisation for permanent retention purposes.

### Personal and shared mailboxes

One policy to be created.

Plus, an export to PST for the mailboxes of select roles (e.g., Executives) within 30 days of the account being deactivated.

**Policy title/s**      • All staff – 10 years – ‘Do nothing’

**Static or adaptive**      • Static

**Scope**      • One policy - All (personal, shared and resource) mailboxes

**Retention period and trigger**      • All staff - 10 years after the items were created. **NB formal appraisal must be conducted prior to deletion.**

**Action at end of retention**      • Do nothing

**‘Do nothing’ outcomes**      • Active mailboxes: Items can be soft deleted by end users but they will remain stored in a hidden folder of the mailboxes until they cease to be subject to the retention hold, then they will be permanently deleted.  
• Inactive mailboxes: Items already deleted will be permanently deleted over time when they cease to be subject to a retention hold. Items that remained in the mailbox when it was deactivated will remain in place.

**Note:** Inactive mailboxes will be automatically destroyed 30 days after the last item stored is subject to a retention hold.

**Recommended public office actions at the end of the retention period**

- For the majority of mailboxes of departed staff, no action is required. The content will remain discoverable and the mailboxes will be automatically deleted when the last item in the mailbox ceases to be subject to the retention 'hold'. In practice, this means that mailboxes will be retained for 10 years (based on the last email date) after the account is deactivated, then automatically deleted.
- Export selected mailboxes to PST files within 30 days of an account being deactivated (see below)

**Process to export a mailbox to PST for executive plus select mailboxes**

- Set up a new Content Search in the eDiscovery area in Purview.
- In 'Locations', select the mailbox to be exported. In 'Conditions', do not refine the search unless there is a need to do so (for example, by date range, or to define 'Message kind equals email'). Submit the query.
- When the search concludes, select 'Actions' – 'Export results'.

## Retention policy/ies for OneDrive

One retention policy is recommended for executive plus selected OneDrives. Any State records stored within OneDrive must be moved to and managed in a more appropriate location.<sup>68</sup>

Note that Microsoft began charging for the storage of inactive OneDrives from late January 2025.<sup>69</sup>

### OneDrive

One policy to be created for selected staff only, to be retained for 10 years with the 'Do nothing' action selected. (All other OneDrives will be covered by the 93 day Recycle Bin retention and back-ups if required).

**Policy title**

- OneDrives – Executive and selected users – 10 years

**Static or adaptive**

- Static, unless the organisation has E5 licences and decides to use adaptive policies

**Scope**

- One policy – Executive and selected users

**This may be varied as required**

<sup>68</sup> Records should not be stored in OneDrive and public offices should ideally limit their size and monitor their use. If, however, OneDrive is used as part of an public office's recordkeeping system, a policy outlining the use and disposal process should be developed.

<sup>69</sup> **Source:** [Manage unlicensed OneDrive user accounts - SharePoint in Microsoft 365 | Microsoft Learn](#) (accessed 2 May 2025)

**Retention period and trigger**

- 10 years after the items were modified. **NB formal appraisal must be conducted prior to deletion.**

**Action at end of retention**

- Do nothing

**'Do nothing' outcomes**

- Active OneDrives: Items can be soft deleted by end users but they will remain stored in the OneDrive Preservation Hold library until they cease to be subject to the retention hold, then they will be permanently deleted.
- Inactive OneDrives: Items already deleted will be permanently deleted over time when they cease to be subject to a retention hold. Items that remained in the OneDrive when it was deactivated will remain in place.

**Note:** Inactive OneDrives will be automatically destroyed 93 days after the last item stored is subject to a retention hold.

**Recommended public office actions at the end of the retention period**

- For the majority of OneDrives of departed staff that are not subject to any retention policy, no action is required. The OneDrive will be automatically destroyed.
- For select OneDrives, no action is required. The content will remain discoverable and the OneDrive will be automatically deleted when the last item stored in it ceases to be subject to the retention 'hold'. In practice, this means that (a) these OneDrives will be retained for 10 years, based on the date the last item was modified, after the account is deactivated, then automatically deleted. The OneDrive will be automatically 'archived' by Microsoft and the public office will be billed for this storage.

---

## Retention policy/ies for Microsoft 365 Groups (Exchange mailbox and SharePoint site)

The retention policy for Microsoft 365 Groups applies to all items in the Group's mailbox and SharePoint site.

Note: This policy does not apply to standard<sup>70</sup> channel messages of any Team linked with the Group. See retention policy/ies for Teams channels below for retention policy for teams chats.

---

### Microsoft 365 Groups

A policy for all Microsoft Groups to be retained for 10 years with a 'Do nothing' action selected

**Policy title/s**

- All Microsoft 365 Groups – 10 years – Do nothing

---

<sup>70</sup> Microsoft define a Teams 'standard channel' as one that 'is visible and accessible to all team members.' Private channels, on the other hand, are only visible to a sub-set of the team.

<b>Static or adaptive</b>	<ul style="list-style-type: none"> <li>• Static, unless the organisation has E5 licences and decides to use adaptive policies</li> </ul>
<b>Scope (Three options shown)</b>	<ul style="list-style-type: none"> <li>• One policy - All Microsoft 365 Groups</li> <li>• Multiple policies - A combination of Microsoft 365 Groups, 'included' or 'excluded' manually. For example, Groups used to store short-term temporary content may be excluded.</li> <li>• One policy – Using adaptive policies</li> </ul>
<b>Retention period and trigger</b>	<ul style="list-style-type: none"> <li>• 10 years after the items were modified. <b>NB formal appraisal must be conducted prior to deletion.</b></li> </ul>
<b>Action at end of retention</b>	<ul style="list-style-type: none"> <li>• Do nothing</li> </ul>
<b>'Do nothing' outcomes</b>	<ul style="list-style-type: none"> <li>• Any deleted items in the Group's mailbox or SharePoint site will be automatically deleted when they cease to be subject to a retention hold.</li> <li>• All other items will remain in place until the Group's resources are subject to a formal disposal process.</li> </ul>
<b>Recommended public office actions at the end of the retention period</b>	<ul style="list-style-type: none"> <li>• Public offices will need to establish a method to identify what Groups are subject to a retention policy and when retention policies cease to apply to items in the Group's SharePoint site and mailbox. Monitoring when sites become inactive will help to support this process.</li> <li>• Public offices will need to establish a process to appraise and dispose of (or extend the retention for) items stored in the Group's SharePoint site.</li> </ul>

## Retention policy/ies for non-Group-based SharePoint sites

This retention policy applies to all SharePoint communication sites and non-Group-based sites. This includes SharePoint sites linked with Teams private and shared channels but not the message-based content of the private or shared channel; these are subject to Teams retention policies – see below.

### Non-Group SharePoint sites

A policy for non-group SharePoint sites to be retained for 10 years with a 'Do nothing' action selected

**Policy title**

- Non-Group SharePoint sites – 10 years – Do nothing

**Static or adaptive**

- Static, unless the organisation has E5 licences and decides to use adaptive policies

**Scope (Three options shown)**

- One policy - All SharePoint sites
- Multiple policies - A combination of SharePoint sites, 'included' or 'excluded' manually

---

	<ul style="list-style-type: none"> <li>• One policy – Using adaptive policies</li> </ul>
<b>Retention period and trigger</b>	<ul style="list-style-type: none"> <li>• 10 years after the items were modified. <b>NB formal appraisal must be conducted prior to deletion.</b></li> </ul>
<b>Action at end of retention</b>	<ul style="list-style-type: none"> <li>• Do nothing</li> </ul>
<b>‘Do nothing’ outcomes</b>	<ul style="list-style-type: none"> <li>• Any deleted items in the SharePoint site will be automatically deleted when they cease to be subject to a retention hold.</li> <li>• All other items will remain in place until the SharePoint site is subject to a formal disposal process.</li> </ul>
<b>Recommended public office actions at the end of the retention period</b>	<ul style="list-style-type: none"> <li>• Public offices will need to establish a method to identify what non-Group SharePoint sites are subject to a retention policy and when retention policies cease to apply to items in the SharePoint site. Monitoring when sites become inactive will help to support this process.</li> <li>• Public offices will need to establish a process to appraise and dispose of (or extend the retention for) items stored in the SharePoint site.</li> </ul>

---

## Retention policy/ies for Teams chats

This retention policy applies to the compliance copies of Teams 1:1 and 1:many chats that are stored in a hidden folder in personal Exchange Online mailboxes.

- Teams chats and Copilot interactions were previously subject to a single policy but there are now (or will be soon) separate policies for Copilot experiences and Enterprise AI apps.<sup>71</sup>

Teams chats may be seen as either: (a) ephemeral records that can be destroyed within a short period or (b) content that needs to be retained for as long as the mailbox in which the ‘compliance copies’ are stored. For most NSW government public offices, they will likely fall into the second category.

**Note:** Teams chats can contain critical evidence of public office decision making. If they remain in Teams chats, it is possible that a public office will not be complying with the Create, Capture and Control standard due to the inability to export or capture Teams chats in recordkeeping systems.

---

### Teams chats

A policy for teams chats to be retained for 10 years with a ‘Destroy automatically’ action selected

- |                     |  |
|---------------------|--|
| <b>Policy title</b> | <ul style="list-style-type: none"> <li>• Teams chats – 10 years – Destroy automatically</li> </ul> |
|---------------------|--|
- 

<sup>71</sup> Microsoft advise that the separate options ‘are rolling out and may not yet be visible in your Purview tenant’ and has provided guidance on how to separate existing legacy policies. **See** [Automatically retain or delete content by using retention policies | Microsoft Learn \(accessed 2 May 2025\)](#) and [Learn about retention for Copilot and AI apps | Microsoft Learn \(accessed 2 May 2025\)](#).

<b>Static or adaptive</b>	<ul style="list-style-type: none"> <li>• Static, unless the organisation has E5 licences and decides to use adaptive policies</li> </ul>
<b>Scope</b>	<ul style="list-style-type: none"> <li>• All messages from individual chats, group chats, meeting chats, bot chats.</li> </ul>
<b>Retention period and trigger</b>	<ul style="list-style-type: none"> <li>• 10 years after date created (in line with the mailbox in which they are stored)</li> </ul>
<b>Action at end of retention</b>	<ul style="list-style-type: none"> <li>• Delete automatically</li> </ul>
<b>'Delete automatically' outcomes</b>	<ul style="list-style-type: none"> <li>• Any chats deleted by an end user will remain stored in a hidden folder of their mailbox; the copy in the mailboxes of other participants will remain unless they are deleted. The deleted items will be automatically deleted when they cease to be subject to a retention hold. Note that an end user deletion action only deletes their copy.</li> <li>• For all chats (deleted or not), the compliance copy of the chat will be automatically deleted from the hidden folder of the end user's mailbox when the chat ceases to be subject to a retention hold. This process triggers an action in the Azure Cosmos database to delete the 'master' copy. This action is permanent and irreversible.</li> </ul>
<b>Recommended public office actions at the end of the retention period</b>	<ul style="list-style-type: none"> <li>• No action is possible, the items will be deleted automatically.</li> <li>• Public offices should consider monitoring the volume of Teams chats in either the Microsoft 365 admin centre or the Teams admin centre.</li> </ul>

## Retention policy/ies for Microsoft Copilot experiences

This retention policy applies to the compliance copies of messages created by Microsoft Copilot experiences and Copilot Studio that are stored in a hidden folder in personal Exchange Online mailboxes.

### Microsoft Copilot experiences

A policy for Copilot experiences to be retained for 10 years with a 'Destroy automatically' action selected

**Policy title**      • Microsoft Copilot experiences –10 years – Destroy automatically

**Static or adaptive**      • Static

**Scope**      • All messages from all Microsoft Copilot experiences.

**Retention period and trigger** • 10 years after date created (in line with the mailbox in which they are stored)

**Action at end of retention** • Delete automatically

**'Delete automatically' outcomes** • Copilot experiences are stored in a hidden folder of user mailboxes. They will be automatically deleted when they cease to be subject to a retention hold.

**Recommended public office actions at the end of the retention period** • No action is possible, the items will be deleted automatically.

---

## Retention policy/ies for Enterprise AI apps

This retention policy applies to the compliance copies of messages created by Enterprise AI apps such as ChatGPT Enterprise that are stored in a hidden folder in personal Exchange Online mailboxes.

---

### Enterprise AI apps

A policy for Enterprise AI apps to be retained for 10 years with a 'Destroy automatically' action selected

**Policy title** • Enterprise AI apps – 10 years – Destroy automatically

**Static or adaptive** • Static

**Scope** • All messages from all Enterprise AI apps.

**Retention period and trigger** • 10 years after date created (in line with the mailbox in which they are stored)

**Action at end of retention** • Delete automatically

**'Delete automatically' outcomes** • Enterprise AI apps messages are stored in a hidden folder of user mailboxes. They will be automatically deleted when they cease to be subject to a retention hold.

**Recommended public office actions at the end of the retention period** • No action is possible, the items will be deleted automatically.

## Retention policy/ies for Teams (standard and shared) channel posts

The retention policy for Teams standard\* and shared channel posts applies to the compliance copy of these posts that are stored in a hidden folder in the Group's mailbox. For this reason, it is recommended that these posts are retained for the same period as the retention period applied to the Group.

\*Microsoft define a Teams 'standard channel' as one that 'is visible and accessible to all team members.'<sup>72</sup> Private channels, on the other hand, are only visible to a sub-set of the team.

---

### Teams standard and shared channel posts

A policy for teams standard and shared channel posts to be retained for 10 years with a 'Do nothing' action selected

<b>Policy title</b>	<ul style="list-style-type: none"><li>• Teams standard and shared channel posts – 10 years – Do nothing</li></ul>
<b>Static or adaptive</b>	<ul style="list-style-type: none"><li>• Static, unless the organisation has E5 licences and decides to use adaptive policies</li></ul>
<b>Scope</b>	<ul style="list-style-type: none"><li>• One policy – Messages from (standard and shared) channel conversations and channel meetings.</li></ul>
<b>Retention period and trigger</b>	<ul style="list-style-type: none"><li>• 10 years after the items were created</li></ul>
<b>Action at end of retention</b>	<ul style="list-style-type: none"><li>• Do nothing</li></ul>
<b>'Do nothing' outcomes</b>	<ul style="list-style-type: none"><li>• Any channel messages deleted by an end user will remain stored in a hidden folder of the Group's mailbox and will then be automatically deleted when they cease to be subject to a retention hold.</li><li>• The compliance copy of all non-deleted channel messages will remain stored in the hidden folder of the Group's mailbox until the Group is deleted.</li><li>• This process triggers an action in the Azure Cosmos database to delete the 'master' copy of all channel messages. This action is permanent and irreversible.</li></ul>
<b>Recommended public office actions at the end of the retention period</b>	<ul style="list-style-type: none"><li>• No action is possible, the items will be deleted automatically.</li><li>• Public offices should consider monitoring Teams content using the AI and Machine Learning (and possibly also eDiscovery) tools in Purview and, where necessary, exporting content (via eDiscovery) that needs to be retained.</li></ul>

---

<sup>72</sup> **Source:** [Standard channels in Microsoft Teams - Microsoft Teams | Microsoft Learn](#) (accessed 2 May 2025)

## Retention policy/ies for Teams private channel posts

Compliance copies of Teams private channel posts are stored in a hidden folder of the personal Exchange mailbox of every member of the private channel. As these are very difficult to access (except via a Content Search or eDiscovery), it is recommended that public offices regard them as ephemeral and seek to ensure that (a) private channels are used for specific reasons only, (b) all chats are ephemeral, and (c) all content stored in the private channel SharePoint site is re-located to the parent Group's site on a regular basis.

---

### Teams private channel posts

A policy for teams private channel posts to be retained for 10 years with a 'Delete automatically' action selected

**Policy title** • Teams private channel posts – 10 years – Delete automatically

**Static or adaptive** • Static, unless the organisation has E5 licences and decides to use adaptive policies

**Scope** • One policy – Messages from Teams private channels

**Retention period and trigger** • 10 years after the items were created

**Action at end of retention** • Delete automatically

**'Delete automatically' outcomes**

- Any private channel posts deleted by an end user will remain stored in a hidden folder of their mailbox and will then be automatically deleted when they cease to be subject to a retention hold. Note that an end user deletion action only deletes their copy.
- For all channel messages (deleted or not), the compliance copy of the chat will be automatically deleted from the hidden folder of the end user's mailbox when the channel message ceases to be subject to a retention hold. This process triggers an action in the Azure Cosmos database to delete the 'master' copy. This action is permanent and irreversible.

**Recommended public office actions at the end of the retention period**

- No action is possible, the items will be deleted automatically.
- Public offices should consider monitoring Teams content using the AI and Machine Learning (and possibly also eDiscovery) tools in Purview and, where necessary, exporting content (via eDiscovery) that needs to be retained.

# Attachment B – Pay-as-you-go subscription services

The details below were correct on 5 May 2025. They may change at short notice.

## SharePoint Advanced Management

SharePoint Advanced Management is a Microsoft 365 add-on that provides the following features.<sup>73</sup> These are set up in the SharePoint admin centre and are in two groups:

- Block download policy for SharePoint and OneDrive - Prevent download for both external and internal users
- Change history - Find who made particular site or organization setting changes and when
- Conditional access policies for SharePoint and OneDrive - Control whether users can access sensitive sites based on conditions like location or operating system
- Data access governance reports - Discover potential oversharing and keep track of sites that have sensitive files
- Default sensitivity labels for document libraries - Help make sure sensitive project files are appropriately labelled
- OneDrive access restriction - Allow only particular groups of users to use OneDrive
- Recent actions - Review recent site changes you made
- Site lifecycle management - Automate tasks across the life cycle of your sites
- Site-level access restriction - Allow admins to restrict access to specific SharePoint sites and their content

## Microsoft Syntex

Microsoft (formerly SharePoint) Syntex provides a series of pay-as-you-go services that are only accessible on top of existing Microsoft 365 licences. Some of these services have the potential to augment the management of records.

The following services were available as of May 2025 (or as indicated, some are in preview).<sup>74</sup>

- Document and image services
  - Autofill columns
    - This option can be used to auto-populate metadata using natural language queries created in a SharePoint library column.
  - Content assembly (automatically generate standard repetitive business documents, such as contracts, etc)
  - Document translation
  - SharePoint eSignature

---

<sup>73</sup> **Source:** [SharePoint Advanced Management overview - SharePoint in Microsoft 365 | Microsoft Learn](#) (accessed 2 May 2025)

<sup>74</sup> **Source:** [Overview of Microsoft Syntex - Microsoft Syntex | Microsoft Learn](#). **For details of the costs, see** [Pay-as-you-go services and pricing for Microsoft Syntex - Microsoft Syntex | Microsoft Learn](#). (both sites accessed 2 May 2025)

- This service provides an alternative to other more well-known e-signature services.
  - Image tagging
    - This option is useful if images with readable text are uploaded as it extracts the text into an 'Image text' column, making it possible to search for those images.
  - Optical character recognition (OCR)
    - Note that OCR only works for newly received items that are stored in SharePoint or OneDrive. It does not 'convert' an existing non-text-based file stored in those locations to a searchable PDF. Instead, the OCR process extracts the data and stores it within a linked but hidden column, making the item 'searchable'.
    - Organisations that want to convert existing or newly received unsearchable PDFs to become searchable PDFs should consider third-party options.
  - Prebuilt document processing (to extract metadata)
  - Structured and freeform document processing (to extract metadata)
  - Taxonomy tagging
    - This service can be used to auto-populate metadata from the Term Store.
  - Unstructured document processing (to extract metadata)
- Storage services
  - Microsoft 365 Archive ('long-term storage for inactive SharePoint content')
  - Microsoft 365 Backup (Preview)
- Video translation services
  - This service can be used to translate transcripts in Stream for SharePoint.
- Other included features
  - Annotations for the following file types - .ai, .dwg, .epub, .pdf, .rtf, and .tiff
    - Content query, to search metadata in document libraries
    - Merge and extract PDFs
    - Processing rules
    - Site templates
- Advanced taxonomy tools
  - This services can be used import taxonomies using SKOS, SKOS formatting reference, push content type to hub, and term store reports.

## AI Builder

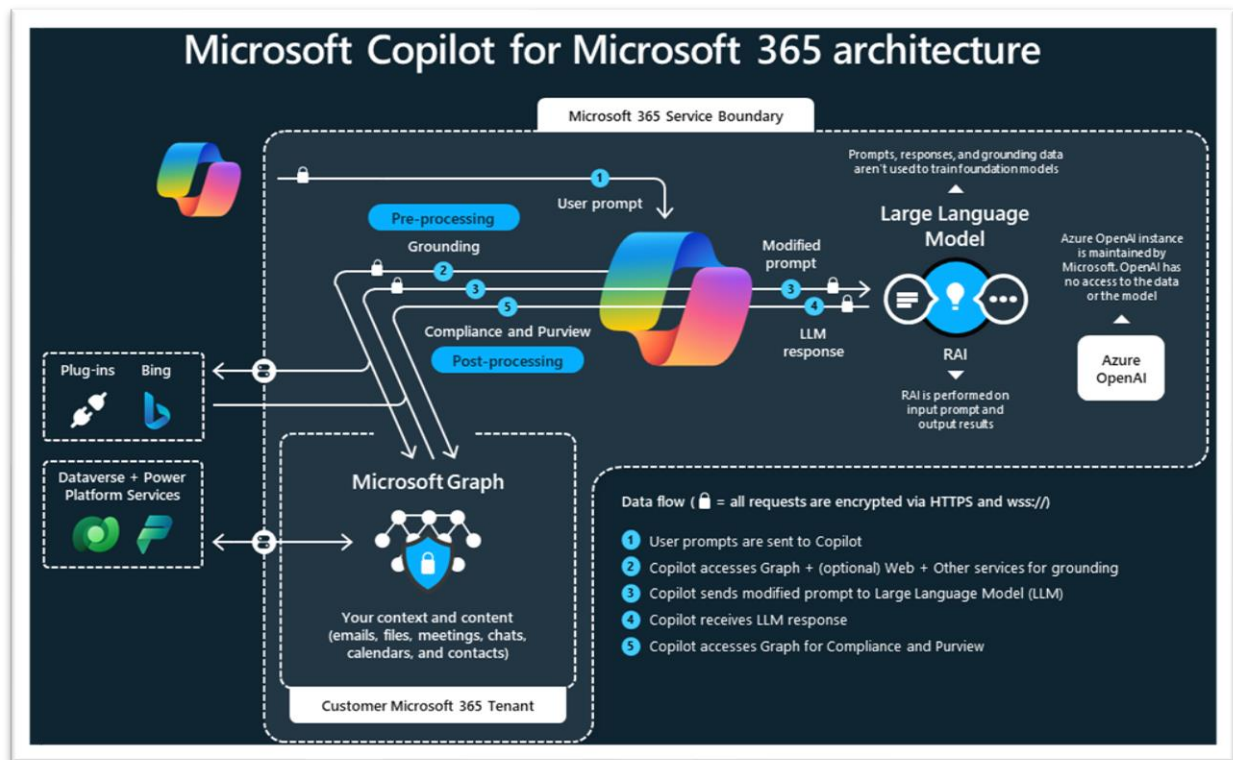
For an overview of AI Builder functionality, some of which links into the underlying AI functionality in Microsoft 365 – see [Overview of AI Builder | Microsoft Learn](#) (accessed 2 May 2025)

## Copilot

According to the online documentation, 'Microsoft Copilot for Microsoft 365 is an AI-powered productivity tool that coordinates large language models (LLMs), content in Microsoft Graph, and the Microsoft 365 productivity apps that you use every day, such as Word, Excel, PowerPoint, Outlook, Teams, and others. This integration provides real-time intelligent assistance, enabling users to enhance their creativity, productivity, and skills.

Copilot for Microsoft 365 uses a combination of LLMs, a type of artificial intelligence (AI) algorithm that uses deep learning techniques and vast data sets to understand, summarize, predict, and generate content. These LLMs include pre-trained models, such as Generative Pre-Trained Transformers (GPT) like GPT-4, designed to excel in these tasks.<sup>75</sup>

The image below (from the link in the footnote referenced in the previous paragraph) provides summary details describing where Copilot gets its information from.



*Image: Microsoft Copilot for Microsoft 365*

Organisations intending to use Copilot for the capture, creation or management of records should familiarize themselves with guidance about artificial intelligence (AI) and recordkeeping provided by State Records NSW.<sup>76</sup>

<sup>75</sup> **Sources:** Microsoft Copilot for Microsoft 365 overview | Microsoft Learn, Data, Privacy, and Security for Microsoft Copilot for Microsoft 365 | Microsoft Learn (accessed 2 May 2025)

<sup>76</sup> **See:** Artificial intelligence and public office recordkeeping | NSW Government (accessed 5 May 2025)

# Attachment C – Microsoft 365 admin centres

The following is a list of the sections in the various Microsoft 365 admin centres. Sections that include settings relating to the management of records are described in the body of the document.

## Microsoft Entra / Azure Active Directory admin centre

- Identity
  - Users
    - All users
    - Deleted users
    - User settings
  - Groups
    - All groups
    - Deleted groups
    - Group settings
  - Devices
    - All devices
    - Bitlocker keys
  - Applications
    - Enterprise applications
    - App registrations
  - Roles & Admins
    - Roles & Admins
    - Admin units
    - Delegated admin partners
  - Billing
    - Licences
    - Linked subscriptions
  - Settings
    - Preview hub
    - Domain names
    - Mobility
  - Protection
    - Identity Protection
    - Conditional Access
    - Security Centre
    - Identity Secure Score

## Multifactor authentication

- Authentication methods
- Password reset
- Custom security attributes
- Risky activities
- Identity Governance
  - Entitlement management
  - Access reviews
  - Privileged Identity Management

- Lifecycle workflows
- External Identities
  - All identity providers
  - User flows
  - Custom authentication extensions
  - Cross-tenant access settings
  - External collaboration settings
  - Cross-tenant synchronization
- User experiences
  - Company branding
- Hybrid Management
  - Microsoft Entra Connect
- Monitoring & Health
  - Sign-in logs
  - Audit logs
  - Provisioning logs
  - Health
  - Log analytics
  - Diagnostic settings
  - Workbooks
  - Usage & insights
  - Bulk operations
- Permissions Management
- Global Secure Access

## Microsoft 365 Admin centre

- Users
  - Active users
  - Contacts
  - Guest users
  - Deleted users
- Teams & Groups
  - Active teams & groups
  - Policies
  - Deleted groups
  - Shared mailboxes
- Roles
  - Role assignments
- Administrative units
  - Resources
    - Rooms & equipment
    - Sites
  - Billing
    - Purchase services
    - Your products
    - Licences
    - Bills & payments
    - Billing accounts
    - Payment methods
    - Billing notifications

Support

- Help & support
  - View service requests
  - Customer Lockbox Requests
  - Microsoft Surface support
- Settings
  - Domains
  - Search and Intelligence
  - Org Settings
    - Services (tab)
    - Security and Privacy (tab)
    - Organisation profile (tab)
  - Microsoft 365 Backup
  - Integrated apps
  - Viva
  - Partner relationships
  - Microsoft Edge
- Set up
- Reports
  - Adoption score
  - Usage
  - Organisational messages (Preview)
- Health
  - Service Health
  - Message centre
  - Product feedback
  - Network connectivity
  - Software updates
- Exchange Online
  - Recipients
    - Mailboxes
    - Groups
    - Resources
    - Contacts
  - Mail flow
    - Message trace
    - Rules
    - Remote domains
    - Accepted domains
    - Connectors
    - High Volume Email (Preview)
    - Alerts
    - Alert policies
  - Roles
    - Admin roles
    - User roles
    - Outlook web app policies
  - Migration
  - Mobile
    - Mobile device access
    - Mobile device mailbox policy
  - Reports
    - Mail flow

- Migration
  - Outlook for Windows Usage
- Insights
- Public folders
- Organisation
  - Sharing
- Settings
- Troubleshoot
- Other Features

## MS Teams

- Teams Premium
- Settings and policies
  - Teams & channels (Team templates, Preview features, Migrating to Teams),
  - External collaboration (Guest access)
  - Apps (App setup)
  - Meetings & events (Audio conferencing, Meetings, Themes and customisation, Live events, Meeting templates, Events)
  - Messaging
  - Voice (multiple options relating to calling)
  - Emergency (calling and call routing)
  - Enhanced encryption
- Teams
  - Manage teams
  - Team templates
- Users
  - Manage users
  - External access
- Teams devices
  - Teams Rooms on Windows
  - Teams Room on Android
  - Surface Hubs (Legacy)
  - Panels
  - Phones
  - Displays
  - SIP devices
- Teams Apps
  - Manage apps
  - Permission policies
  - Setup policies
  - Customize store
- Meetings
  - Meeting templates
- Voice (multiple options)
- Locations (multiple options)
- Frontline deployment
- Policy packages
- Planning
- Analytics and reports
  - Usage reports
  - Reporting labels

- Call quality dashboard
- Notifications & alarms
  - Rules

## SharePoint Online admin portal

- Active sites
- Containers
  - Active containers
  - Deleted containers
- Policies
  - Sharing
  - Access control
- Settings
  - Includes Classic settings
- Content services
  - Term Store
  - Content type gallery
- Migration
- Reports
  - Data access governance
  - OneDrive accounts. Important - to see which OneDrives may be subject to paid storage.
- Advanced
  - API access
- More features
- Advanced management (Pro)
  - Block download policy for SharePoint and OneDrive
  - Change history
  - Conditional access policies for SharePoint and OneDrive
  - Data access governance reports
  - Default sensitivity labels for document libraries
  - OneDrive access restriction
  - Recent actions
  - Site lifecycle management
  - Site-level access restriction

## Purview

- Audit
  - Communication compliance
  - Compliance alerts
  - Compliance Manager
  - Data Catalog
  - Data lifecycle management
    - Retention policies
    - Retention labels
    - Priority cleanup (preview)
    - Exchange (legacy)
    - Classifiers
    - Explorers
  - Data Loss Prevention
    - Policies
    - Alerts

- Classifiers
  - Explorers
- Data Security Investigations (Preview)
- Data Security Posture Management (Preview)
- DSPM for AI
- eDiscovery
  - Information Barriers
  - Information Protection
  - Insider Risk Management
- Records Management
  - File plan (for retention labels)
  - Policies
    - Label policies
    - Policy lookup
  - Events
  - Disposition
  - Classifiers
  - Explorers
- Settings

## Additional resources

### Government:

[Functional Requirements for Managing Records in Microsoft 365 \(ADRI/CAARA, October 2021\)](#)

[Standard on records management | NSW Government](#)

[ASD's Blueprint for Secure Cloud](#)

### Microsoft:

[Microsoft 365 documentation | Microsoft Learn](#)

[Browse all courses, learning paths, and modules - Training | Microsoft Learn](#)

### Blogs:

[Records about the world – A blog about managing records and information especially in Microsoft 365 \(Andrew Warland, Australia\)](#)

[SharePoint best practices, tips and tricks | SharePoint Maven \(Greg Zelfond, United States\)](#)

[Joanne C Klein – Compliance in Microsoft 365 \(Joanne Klein, Canada\)](#)