



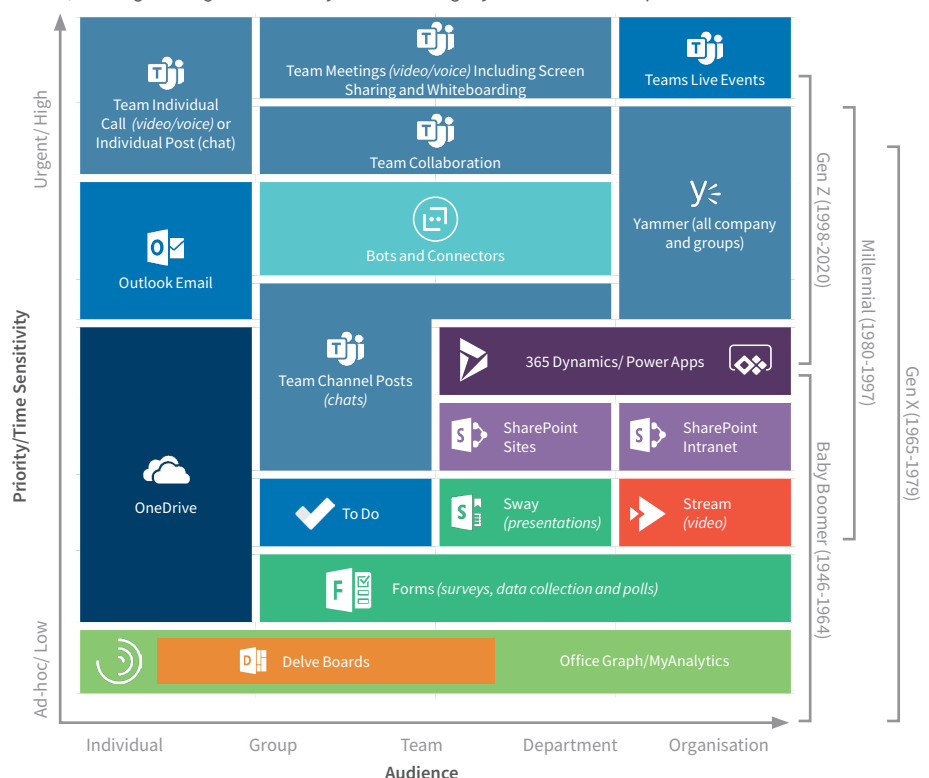
Establishing Information Governance Best Practices for Microsoft 365 Deployments

Microsoft accounts for 92% of the content services market,¹ with most organisations utilising services within Microsoft 365 and/or Microsoft Teams to enable productivity and efficient remote working. In 2020, Microsoft 365 users generated more than 30 billion collaboration minutes in a single day as people communicated, collaborated and created documents at accelerating speed.² This pace of adoption and scale of use has made it difficult for many organisations to maintain consistent information governance (IG).

Widespread use of any enterprise application without sound governance and education can quickly become a slippery slope of data risks. This paper will discuss the range of Microsoft 365 productivity and collaboration applications available and share how organisations can align IG best practices as their content services deployments evolve.

Understanding what applications are available within Microsoft 365 and how they interact with the broader organisation is integral to maintaining visibility into where critical business records are being generated and the controls needed to manage that data in accordance with information governance and compliance requirements. Figure 1 illustrates the core Microsoft 365 applications and uses for each application.

FIGURE 1
Microsoft 365 Applications - What to Use and When. *Note: Office 365 Groups have been replaced by Teams; although an organisation may still have a legacy of Office 365 Groups*



Based on Avanade graphic 2016 and updated for M365 2020

¹ Google's G Suite is no Microsoft killer, but still winning converts, 1 February 2018

² Microsoft Teams reaches 115 million DAU—plus, a new daily collaboration minutes metric for Microsoft 365, 28 October, 2020

Against this backdrop of potential features in use, there are three key areas in which IG opportunities and best practices may need to be addressed or strengthened: messaging, collaboration and data management. In this section, we’ll look at these areas and how organisations can optimise deployments and user education to improve information governance enterprise wide.




1. Messaging

Users have multiple ways to communicate within Microsoft 365 – with each mode designed for specific purposes. This provides an opportunity for organisations to reset and establish more effective and secure communications practices. It requires a combination of user education and embedding information governance rules within Microsoft 365 to support compliant behaviour and track and manage missteps.

	METHOD	WHAT TO USE WHEN	VALUE	GOOD PRACTICES	RISKY PRACTICES
External	 External Social Media	Customer / public-wide communications	High (Records) ★ ★ ★	<ul style="list-style-type: none"> Following corporate policy and defined approach to managing external corporate social media as records. 	<ul style="list-style-type: none"> Sharing personal data on social media.
Internal (M365 Messaging Applications)	 Email	Official external and internal communications (Team to External)	Medium (Operational) ★ ★ ☆	<ul style="list-style-type: none"> Using email for official communications only and using other channels for less formal discussions to reduce email overload. 	<ul style="list-style-type: none"> Storing important emails (<i>record of decisions</i>) in Outlook folders, they can be lost and maybe an essential part of a record.
	 Internal Social Media (Post)	Department to organisation-wide communication		<ul style="list-style-type: none"> Saving important emails to a corporate record repository keeps all documents related to a decision (<i>a record</i>) together. 	<ul style="list-style-type: none"> Sending documents for review as attachments internally creates duplication, version history issues and adds to storage.
	 Team Chat (Post)	Group (team) communications and collaboration		<ul style="list-style-type: none"> Sending links when collaborating internally reduces duplication and is a more secure way to collaborate. 	<ul style="list-style-type: none"> Sending sensitive information externally unencrypted, the data may be “hacked”.
	 Individual Chat (Post)	Individual, casual communications	Low (Transient) ★ ☆ ☆	<ul style="list-style-type: none"> Using encryption when sending information confidential or above externally to keep it secure. Using Teams chat (<i>posts</i>) to enable quicker and more effective collaboration around files and activities across your team keeps files and discussions in one searchable place. Putting technical controls in place to help manage the compliant handling of messages, such as DLP rules and tips. 	<ul style="list-style-type: none"> Using chat to send sensitive information to a colleague, the data may be visible to other colleagues.

2. Collaboration and Storage















Microsoft 365 provides powerful and versatile collaboration and storage solutions. Each enables a unique set of capabilities. Often, business users begin using these applications without a clear awareness of what to use, when and why or the legal and compliance implications that can result if they are not used within the bounds of IG policy. Conversely, aligning these collaboration and storage tools with governance delivers improvements in multiple areas such as data risk, storage cost, resilient data, efficiency and time saving. To understand the best practices in Microsoft 365 collaboration and storage capabilities, let’s look at each application in detail:

	METHOD	WHAT TO USE WHEN	VALUE	GOOD PRACTICES	RISKY PRACTICES
Microsoft 365 Applications	 SharePoint	Enterprise / Departmental working <i>(for more complex/ bespoke requirements using M365)</i>	High <i>(Records)</i> ★★ ★	<ul style="list-style-type: none"> ✔ Using SharePoint for more advanced business requirements that require integration with other systems. ✔ Using Libraries and Folders in SharePoint/ Channels in Teams to structure content around activities and Records classification. ✔ Synchronising SharePoint/Team Folders to enable offline working. ✔ Using in-built version control, rather than create new files for each version. ✔ Labelling files as you create and save them <i>(retention and sensitivity)</i>. ✔ Building an Attestation process to routinely review the need and access for Teams and SharePoint Applications. 	<ul style="list-style-type: none"> ⚠ Ad-hoc deletion of Teams or SharePoint Sites without defined retention policies. <i>(Retention needs to be applied to ensure records are retained where required for business, regulation or litigation).</i>
	 Teams	Team (<i>Shared</i>) working	Medium-High <i>(Operational & Records)</i> ★★ ☆	<ul style="list-style-type: none"> ✔ Using Teams to support basic collaboration requirements for Teams and Projects. ✔ Using the Teams add-ins (<i>Tabs</i>) to help improve productivity and share important information/ processes with your team. 	<ul style="list-style-type: none"> ⚠ Allowing Teams or SharePoint Apps to be created within your organisation with no governance or controls in place. <i>(Data quickly becomes ungoverned, generating data risks and costs).</i>
	 OneDrive	Individual working	Low <i>(Non-Records)</i> ★ ☆ ☆	<ul style="list-style-type: none"> ✔ Using OneDrive to keep information that is only pertinent to you as an individual <i>(i.e., it has no corporate value)</i>. 	<ul style="list-style-type: none"> ⚠ Storing business critical or sensitive personal data in OneDrive. ⚠ Drafting on your Desktop or in OneDrive, if you intend to share starting in Teams or SharePoint. This results in the copies of uncontrolled data or data of corporate value.

3. Securing and Managing Data

Microsoft 365 provides robust data security and compliance features; however, many organisations aren't aware of these capabilities and/or do not know how to implement them. Implementing these capabilities helps manage and reduce data risk and provides valuable insights into how data is being used. In turn, these insights can enhance data value and governance.

Microsoft 365's security and compliance features include sensitivity and retention labelling, encryption, Data Loss Prevention (DLP) and the ability to detect and label sensitive data automatically. These features, if used, can help lower the risk of data breaches, enable secure sharing of documents and support business users in handling data appropriately.

	FEATURE	DESCRIPTION	GOOD PRACTICES	RISKY PRACTICES
Microsoft 365 Security and Compliance Features	 Information governance  Records management	<p>These are currently two features in M365 Security and Compliance:</p> <p>Data lifecycle management focuses on providing a simple way to keep the data you want and delete what you don't.</p> <p>Records management: is geared towards meeting the record-keeping requirements of your business policies and external regulations using Retention Labels, Policies and File plan.</p>	<ul style="list-style-type: none">  Aligning the File plan in M365 to your organisation's Records retention schedule to help govern and manage retention rules across M365.  Simplifying the number of labels and complexity of triggers where possible working with your compliance team(s), business and/or data owners to ensure you remain compliant.  Developing an approach to applying Retention labels that are user-focused and, if possible transparent to the user (reducing training burden and making it easy to do the right thing). One size does not necessarily fit all. 	<ul style="list-style-type: none">  Rolling out M365 User Applications without having a strategy on how to apply M365 data lifecycle/records management (you can use labels retrospectively, but this can create more work and disruption).  Providing users with a long list of retention labels to select from to apply (they will invariably click the first one on the list).
	 Information protection	<p>Information Protection helps discover, classify and protect sensitive information wherever it lives or travels.</p>	<ul style="list-style-type: none">  Aligning the M365 sensitivity labels to your organisation's security classification policies and standards. 	<ul style="list-style-type: none">  Rolling out M365 User Applications without having a strategy on how to apply M365 Information Protection (sensitivity labels). You can use labels retrospectively, but this can create more work and disruption).
	 Data loss prevention	<p>Data loss prevention (DLP) is an intelligent service that's part of Microsoft Office 365. It looks for messages, files and documents that contain sensitive information and applies the policies you configure about what can and cannot be done with that data. DLP currently supports the creation of DLP policies, with alerting and Endpoint DLP settings.</p>	<ul style="list-style-type: none">  Automating the enforcement of policies and application of labels, for example encrypting documents that are marked strictly confidential when emailing to an external domain. 	<ul style="list-style-type: none">  Not providing controls to help business users handle data appropriately according to its security classification.  Putting in controls that are too rigid that encourage users to follow non-official routes (shadow IT).

Governance Benefits

IG provides extensive benefits including reduced risk, cost savings and improved efficiencies across all enterprise systems. Applying appropriate governance rules and controls within Microsoft 365 can deliver benefits, including:

Cost Savings



When data is governed correctly, the management and searching of the “data footprint” in a data subject access request (DSAR) under GDPR or other data protection regulation are significantly reduced. Properly governed messaging applications that mitigate data volumes can deliver cost savings in storage, DSAR response and e-discovery/ document review and storage costs.

IMPACT: *Cost* - Legacy systems cost on average 60-80% of IT budgets.

Reduced Risks



Reduced data breach risk through the use of controls to mitigate data leakage, education through DLP hints and tips and reduced footprint of data stored in messaging tools.

IMPACT: *Data Breach* - 68% of those surveyed had sent work emails to the wrong recipient.

Improved Productivity



Improved productivity through more effective communication across business activities, enabling faster access to relevant data to support business processes and decision making.

IMPACT: *Productivity* - Information workers save four hours per week from improved collaboration and information sharing.³

FTI Technology’s Information Governance, Security & Privacy experts have deep experience helping clients align information governance policies to Microsoft 365 and any other enterprise system. Our expertise and knowledge spans developing and establishing Microsoft 365 controls that support governance policies, reinforce training and align technical needs to reduce organisational risk.

Take our quick [Microsoft 365 Information Governance Interactive Assessment](#) to find out how your organisation can improve governance and compliance within Microsoft 365 deployments. FTI Technology provides a range of services that can be tailored to support your M365 Information Governance requirements – see our [Microsoft 365 Information Governance Solutions for Microsoft 365 Service Sheet](#) for more details.

³ Forrester Total Economic Impact™ Of Microsoft Teams

PETER SHARDLOW

Managing Director
+44 (0) 7929 827812
peter.shardlow@fticonsulting.com

JAVIER GARCÍA CHAPPELL

Managing Director
+34 600 83 76 28
javier.garcia-chappell@fticonsulting.com