Fact Sheet October 2022

Microsoft 365 platforms and agencies' compliance obligations

Who is this information for?	NSW public sector agencies seeking guidance on compliance with NSW information access and privacy legislation as it related to the use of Microsoft 365.
Why is this information important to them?	This fact sheet will assist agencies in understanding compliance obligations and considerations when using Microsoft 365 platforms.

This fact sheet aims to provide guidance on the increasing use of Microsoft 365 platforms by public sector agencies, and the impact on agencies' compliance obligations under the *Government Information (Public Access) Act 2009* (GIPA Act); *Privacy and Personal Information Protection Act 1998* (PPIP Act); and *Health Records and Information Privacy Act 2002* (HRIP Act).

The shift towards digitisation

The COVID-19 pandemic accelerated the shift among agencies from paper-based operations to digital workflows.

With the rise of hybrid working arrangements, workplaces have turned toward digital services, such as Microsoft 365, which offer platforms and applications that facilitate remote collaboration.

While agencies have benefitted from the move towards digitisation, it is important for agencies to continually assess the implementation and use of digital platforms within the framework of their information access and privacy responsibilities.

The use of Microsoft 365 platforms

Microsoft 365's commonly used featured platforms for collaborative work include:

- **Microsoft Teams –** a collaboration and video conferencing platform that acts as a central hub for workplace communications via text chat, voice call, video call, calendar, notes, documents, and apps
- **SharePoint –** a cloud-based content collaboration and management platform where files can be shared and stored
- **OneDrive –** a personal cloud-based storage service.

These platforms are integrated and provide agencies with different avenues for sharing, organising and storing information.

Agencies need to ensure that they are utilising these platforms in a manner consistent with their responsibilities and obligations under the GIPA Act, PPIP Act and HRIP Act.

For example, agencies may wish to examine:

- the way in which searches for documents are being performed
- where documents are being stored, saved or recorded
- how individuals' personal and health information are being stored and accessed
- the sharing and access controls applied to certain Microsoft 365 platforms.

Further, with record-keeping practices playing an important role in an agency's compliance with their obligations under the GIPA Act, PPIP Act and HRIP Act, agencies need to ensure that their use of these platforms are in accordance with their obligations under the *State Records Act 1998*. State Records NSW has published guidance on *Microsoft 365 and Recordkeeping*, which highlights the considerations that agencies must be aware of to achieve compliance with the Standard on Records Management[1] and the *State Records Act 1998*.

Of particular relevance, State Records NSW recommended agencies to consider various strategies and actions, some of which includes:

- Integration of Microsoft 365 platforms with an external recordkeeping systems, such as electronic document and records management systems (EDRMS)

[1] Standard on records management | State Records NSW

- Exporting records out of Microsoft 365 platforms for storage in an external recordkeeping system such as EDRMS
- If recordkeeping is contained within Microsoft 365, declaring the content as a record, so that it may be defined as a record in Microsoft 365.

Good administrative practices enable agencies to demonstrate how decisions are made[2], and as agencies take steps to fulfil these requirements, agencies should have regard to what is a 'record'. In the context of achieving compliance with *Standards on records management* and upholding the objects of the GIPA Act, PPIP Act and HRIP Act, agencies should consider the need to declare and store as records any content generated in the collaborative and often iterative process of arriving at a decision.

Information access considerations

Access to government information under the GIPA Act requires consideration of information in a *record* which means any document or other source of information compiled, recorded or stored in written form or by electronic process.[3] This means that access to government information includes records in electronic or digital format. Relevantly, the IPC has published additional guidance on Digital Records and the GIPA Act to assist agencies.

The *State Records Act 1998* also defines record 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.[4]

Additionally, the *State Records Act 1998* also defines a record in relation to its official nature, not just how it has been created or stored. The Act defines state records as those records which are made or received "…in the course of the exercise of official functions."[5]

Under the GIPA Act, an agency is required to undertake reasonable searches for any government information that is within the scope of an information access application.

With the increased use of Microsoft 365 platforms, agencies should be mindful of the importance of searching for information on Microsoft Teams, SharePoint and OneDrive as relevant to the terms of the particular access request.

In the case of *Wojciechowska v Commissioner of Police* [2020] NSWCATAP 173, the NSW Civil and Administrative Tribunal (NCAT) observed that agencies are generally best placed to assess whether the information requested in an access application exists and is held by them. However, if an agency does not have proper systems, processes and oversight of information stored across all its platforms including on Microsoft 365 platforms, an agency is unlikely to be able to make accurate assessments about the existence of information. As a consequence the agency may not be able to satisfy search requirements prior to determining an access application.

Agencies therefore need to uphold a commitment to:

- having updated policies about the type of information and communications that can be stored and shared on different Microsoft 365 platforms
- clearly advising staff about existing policies related to the use of Microsoft 365 platforms and applications and the storing of information into its records systems
- identifying and consulting with relevant staff members about whether information requested in information access applications is located on Microsoft 365 platforms such as SharePoint, OneDrive or Microsoft Teams
- ensuring that search requests facilitate returns that reflect all platforms in use by the agency in exercising its functions
- ensuring that its records and information management policy supports the agency's activities.

Privacy considerations

Agencies should maintain an awareness of the ways in which Information Protection Principles (IPPs) and Health Privacy Principles (HPPs) are applicable to the use of Microsoft 365 platforms.

In many cases, the use of Microsoft 365 platforms by agencies brings into consideration IPPs and HPPs regarding collection, security, storage, use and disclosure.

The following is intended to provide guidance into the way different use cases of Microsoft 365 platforms by agencies might pose risks regarding privacy principles and is not meant to serve as an exhaustive overview.

Video meetings on Microsoft Teams

Videoconferencing via Microsoft Teams has been employed by agencies as a way of facilitating face-to-face interactions among agency staff members during remote working, and engaging with members of the public online rather than in person.

[2] Good conduct and administrative practice - Guidelines for state and local government - NSW Ombudsman

[3] Clause 10, Schedule 4 GIPA Act
[4] Section 3, *State Records Act 1998*, definition of record
[5] Section 3, *State Records Act 1998*, definition of a State Record

When agencies conduct videoconferences with members of the public, it is important for agencies to bear in mind privacy principles such as IPP 3 (HPP 4) and IPP 4 (HPP 2).

IPP 3 requires agencies to inform a person about the collection of their personal information, and IPP 4 requires agencies to not collect personal information that is excessive.

These principles may be at risk in circumstances where online meetings are being recorded unnecessarily or without the consent of participants. All personal or health information that is collected during a videoconference must be handled in accordance with the IPPs and HPPs. To ensure compliance, it is best practice for agencies to:

- avoid recording online meetings when the consent of all participants has not been provided
- avoid recording meetings when there is no relevant purpose for doing so.

Sharing screens on Microsoft Teams

Sharing screens may serve as an effective way of sharing information with online meeting participants. However, sharing screens can involve certain risks which impact privacy principles such as IPP 10 (HPP 10) and IPP 11 (HPP 11).

IPP 10 imposes limits on the way in which personal information is used by agencies, while IPP 11 stipulates that an agency can only disclose personal information under limited circumstances.

Agencies should note that these principles may be at risk when, for example:

- Sharing an incorrect screen with meeting participants, and that screen displays another person's personal or health information
- Toggling between open screen windows whilst screen-sharing, which may mistakenly reveal another person's personal or health information from the toggled windows
- Application notifications (Microsoft Teams chat messages, Outlook previews) appear on the screen whilst on screen share, inadvertently sharing a person's personal or health information displayed within those notifications.

To avoid risks to the privacy principles, agencies should consider if documents, windows and business systems (e.g. case management applications, databases, etc.) relating to other matters can be closed when using the Microsoft Teams video application.

Storing and sharing files via Microsoft 365 platforms

Storing files on platforms such as SharePoint and OneDrive, and sharing files with colleagues within the same agency via Microsoft Teams, has been adopted by agencies as a convenient method for collecting, organising and sending information. Whilst eliminating some of the inefficiency associated with paper-based storage and postage systems, storing and sharing files digitally still presents risks to compliance with certain privacy principles, such as IPP 5 (HPP 5), as well as IPP 10 and 11.

IPP 5 places an obligation on agencies to store personal information securely.

To ensure that agencies meet this obligation while utilising Microsoft 365 platforms, agencies should ensure that there are clear policies in place which specifies the type of information that can be stored on these platforms, and impose access limitations to certain information.

In terms of avoiding risks to IPP 10 and 11, it is important for agencies to be mindful of whether:

- a whole folder of documents or an individual file is being shared
- the correct recipient has been selected when sharing a document
- a file and/or file link needs to be shared for a fixed period of time or with no end date.

Other resources

Other resources that may be useful on this topic include:

- Fact Sheet - Reasonable searches under the GIPA Act
- Fact Sheet - Tips for reducing data breaches when sending emails
- Fact Sheet - Digital records and the GIPA Act
- Microsoft 365 and Recordkeeping | State Records NSW
- Good administrative practices enable agencies to demonstrate how decisions are made
- Cloud Computing | State Records NSW
- Web and Social Media | State Records NSW
- Fact Sheet - Information Protection Principles (IPPs) for agencies
- Fact Sheet - Health Privacy Principles (HPPs) for agencies

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NOTE: The information in this Fact Sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.