



Privacy Impact Assessment (PIA)

PIA Entry Name: Microsoft Copilot

End User Services Office

NASA Point of Contact: Shane McCaw

Phone Number: 321-210-1660

E-mail: shane.a.mccaw@nasa.gov

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

The National Aeronautics and Space Administration (NASA) Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) NASA collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. NASA publishes its PIAs, as well as its System of Records Notices (SORNs), on the NASA public-facing website, which describes NASA's activities that impact privacy, the authority for collecting personally identifiable information (PII), and the procedures to access and have PII amended or corrected if necessary.

Reviewing Official: Stayce Hoult, Chief Privacy Officer



System Overview:

Microsoft Copilot is an AI-powered digital assistant that aims to provide personalized assistance to users for a range of tasks and activities. Copilot can summarize user's day or week, generate summaries, and analyze contents of documents stored in SharePoint and OneDrive. This will include the M365 productivity apps to include Word, PowerPoint, Excel, OneNote, SharePoint, OneDrive, Teams, and Exchange.

Copilot for M365 is a licensed AI-powered tool for use as a digital assistant. Microsoft 365 Copilot is grounded on users' data, like emails, meetings, and files, data may include PII. Additionally includes Copilot Premium.

Microsoft Copilot Light (M365 Copilot Chat) is a free, limited capability chatbot service. Copilot Chat is AI chat grounded in data from the web and powered by the latest large language models (LLMs). Copilot Chat can't invoke organizational content like files, emails, or chats on its own.

Microsoft Copilot Studio - Copilot Studio is a graphical, low-code tool for building agents and agent flows. It is for use with Power Platform only.

Privacy / Authorities and Other Requirements	
List all legal authorities and/or agreements that permit the collection of privacy information by the project. Explain how these authorities permit the project and the collection of privacy information. If the project collects Social Security numbers, also identify the specific statutory authority allowing it.	<p>Executive. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023)</p> <p><u>Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence</u></p> <p>Executive. Order No. 14,179, 90 Fed. Reg. 1125 (Jan. 23, 2025)</p> <p><u>Removing Barriers to American Leadership in Artificial Intelligence</u></p> <p>Executive Order 14320, <u>Promoting the Export of the American AI Technology Stack</u>, issued by President Donald J. Trump on July 23, 2025, and published by the White House.</p> <p>Executive Order, <u>Preventing Woke AI in the Federal Government</u>, The White House, July 23, 2025</p> <p>Office of Mgmt. & Budget, M-25-21 (Apr. 3, 2025)</p>

	<p><u>Accelerating Federal Use of AI through Innovation, Governance, and Public Trust</u></p> <p>Office of Mgmt. & Budget, M-25-22 (Apr. 3, 2025)</p> <p><u>Driving Efficient Acquisition of Artificial Intelligence in Government</u></p> <p>Office of Mgmt. & Budget, M-24-10 (Mar. 28, 2024)</p> <p><u>Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence</u></p> <p><i>Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (Jan. 26, 2023)</i> National Institute of Standards and Technology</p> <p><u>https://doi.org/10.6028/NIST.AI.100-1</u></p>
The records in the system are covered by an existing published System of Records Notice (SORN).	SORN not required
The SORN Name and Number.	

Privacy Act of 1974 / Uses of the Information	
Records on individuals are or will be routinely retrieved from the system by using individual's name or other unique identifier (e.g., personal account number, UUPIC, SSN, etc. is used to locate information about an individual in the application/website/information system/paper record).	No

Paperwork Reduction Act / Characterization of the Information	
The record/application/website/information system collects information in a standard way (via forms, surveys, questionnaires, etc.) from 10 or more persons (e.g., members of the public and NASA contractors, and grantees).	No

Paperwork Reduction Act / Authorities and Other Requirements	
There is an OMB Control Number.	No
The OMB Control Number.	

Privacy / Characterization of the Information	
Information is collected on the following:	NASA Contractors Government Employees Other
Collection contains the following:	Name Date of birth Device identifiers (pacemaker, hearing aid, etc.) Driver's license number Agency User ID (AUID) Work e-mail address Birth certificate Death certificate Work Mailing Address
The collection is the minimum necessary to accomplish the purpose of the collection.	Yes
Discuss the intra-Departmental sharing of information. Identify and list the name(s) of any components or directorates within the Department with which the information is shared.	Upon review and further analysis of data, M365 Copilot output can be shared among various NASA organizations. Information warranting protection will be handled in accordance with NASA's requirements (NPR 2810.7).

Privacy / Uses of the Information	
NASA will use the information in the following ways:	Stakeholders will use the information in various ways to communicate and enhance assigned tasks This stored data provides users with Copilot activity history in Microsoft 365 Copilot Chat (previously named Business Chat) and meetings in Microsoft Teams . This data is processed and stored in alignment with contractual commitments with your organization's other content in Microsoft 365. The data is encrypted while it's stored and isn't used to train foundation LLMs, including those used by Microsoft 365 Copilot.
The application/website/information system stores, collects, or maintains Information in Identifiable Form (IIF).	Yes

Consent / Notice	
Does the project provide individuals notice prior to the collection of information?	Yes

If no, explain why individuals are not notified prior to collection of information.	
If yes, describe how the notice provided for the collection of information is adequate to inform those impacted.	[Generally] when information is retrieved, users are notified that the information will be used for the purposes for which it was intended and NASA's Terms of Use are followed.
Do individuals have opportunities to decline to provide information, or opt out of the project?	Yes
If yes, describe the process. If this is not an option, explain why not.	n/a various processes depending on condition for which the data was obtained
Do individuals have opportunities to consent to specific/targeted uses of their information?	No
If yes, describe the process. If this is not an option, explain why not	n/a - we are using the data, not collecting the data. Question not relevant for AI.
The IIF is collected	Voluntary
There is a process in place for the following:	
Ensuring consent is obtained from the individuals whose IIF is stored, collected, or maintained.	Yes
Are individuals provided with notice that they have opportunities to consent to uses, decline to provide information, or opt out of the project?	Yes
If yes, describe the process. If no, explain why not.	n/a - various processes depending on condition for which the data was obtained
Are individuals notified of the consequences of providing information?	Yes
If yes, describe the process. If no, explain why not.	notification and consent provided and obtained considering the circumstance for which the information was collected

Data Retention	
Explain how long each type of information is retained. Include a justification for the retention period of each information type and how/why that period is necessary to the mission/project.	Copilot interactions are stored in a hidden folder in the users mailbox in Exchange, which are bound to the Exchange retention policies of 7 years.

Information Sharing	
Is information shared outside of the organization as part of the normal agency operations?	No
Identify who the information is shared with, how the information is accessed, and how it is to be used.	n/a

Describe how the external sharing noted in the previous question is compatible with the SORN noted in PIA-02.	
---	--

Redress	
What are the procedures that allow individuals to access their information?	n/a Any data protected by the Privacy Act adheres to redress processes outlined in applicable SORN.
What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	n/a Any data protected by the Privacy Act adheres to redress processes outlined in applicable SORN.
How does the project notify individuals about the procedures for correcting their information?	n/a Any data protected by the Privacy Act adheres to redress processes outlined in applicable SORN.

Auditing and Accountability	
How does the project ensure that the information is used in accordance with stated practices in this PIA?	NASA follows NIST AI Controls - NASA baseline requirements and NASA critical controls for systems with artificial intelligence (AI) components; CONTROL BASELINES AND CRITICAL CONTROLS FOR NASA INFORMATION SYSTEMS SECURITY CONFIGURATION SPECIFICATION, NASA-SPEC 2661.Controls
Describe what privacy training is provided to users either generally or specifically relevant to the project.	NASA Cybersecurity and Privacy Awareness Training
What procedures are in place to determine which users may access the information and how does the project determine who has access?	AC-02 Account Management AC-03(07) Access Enforcement
How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within the department and outside?	The Authorizing Official (AO) and Information System Owner (ISO) must review Information Sharing Agreements (ISAs).

Security Controls / Characterization of the Information	
Monitor and Response to privacy and/or security incidents policies.	Yes

Security Controls / Auditing and Accountability	
Technical controls (safeguards) are in place to minimize the possibility of unauthorized access, use,	Yes

or dissemination of the IIF in the application/ website/information system/ cloud system.	
Access controls.	Yes

Information Sharing Practices / Characterization of Information	
The application/website/information system/cloud systems collects IIF from other resources (e.g., databases, websites).	Yes
The application/website/information system/cloud system populates data for other resources (e.g., databases, websites, or external agencies, people, or organizations).	Yes

Accessibility, Redress, Complaints / Characterization of the Information	
There is a process in place for periodic reviews of IIF in the system to ensure data integrity, availability, accuracy, and relevance.	No

Web Measurement and Customizing Technology / Characterization of the Information	
The Application/Website/Information System Utilizes Web Measurement and Customization Technology (Cookies/Persistent Tracking).	Yes

Agency Privacy Manager (APM):

Guerin, Michael D
HARRIS HOULT, STAYCE D
Kostka, Paul A
Midulla, Laura P
Scholz, Matthew C

APM Review Decision: Concur

APM Review Date: 11/24/2025

Chief Privacy Officer (CPO):

HARRIS HOULT, STAYCE D

CPO Review Decision: Concur

CPO Review Date: 12/10/2025

CPO Digital Signature

NASA Senior Agency Information Security Officer (SAISO):

Fletcher, Tamiko N

SAISO Review Decision: Concur

SAISO Review Date: 12/10/2025

NASA Senior Agency Official for Privacy (SAOP):

SEATON, JEFFREY M

SAOP Review Decision: Approve

SAOP Review Date: 12/10/2025