University of Minnesota

Self-Help Guide

Gemini: Data and Privacy Guidance

Learn how your data is stored in Gemini and find guidance on privacy, opting out, data collection, and appropriate use of Health Information and student information.

When using Gemini with your University account, you may use University-classified data, including Private-Highly Restricted information, in accordance with applicable privacy, security, and data classification policies. Learn more about data classification.

Data and privacy guidance for Gemini

Privacy and data ownership

Enterprise-grade data protection: What it means for your data

The University of Minnesota prioritizes the privacy, intellectual property, and data security of our community members. Google offers the following conditions when using the Gemini through our UMN login:

- **No data training:** Google will not use your prompts, responses, or any uploaded data to train its public AI models or machine learning algorithms.
- **Data isolation:** All interactions with Gemini are isolated from consumer-facing services. Your data remains strictly within a secure institutional boundary.
- **No commercial exploitation:** Your data is not sold, shared with third parties, or used for advertising purposes without your permission.

- **No internal surveillance of content:** No instructor or faculty member has access to your individual prompt history or the content of your generated responses.
    - However, like all University-provided IT resources, this data is subject to institutional policies and may be accessed by authorized personnel *under specific conditions* such as system maintenance, legal requirements, or investigations into policy violations.

Data that University administrators can access

The University's administrators for Google Workspace for Education, comprising fewer than six members on the Messaging and Calendaring Team, has limited visibility into individual usage to balance operational awareness with strict user privacy. Their admin console provides aggregated metadata rather than granular user activities. The specific metrics available include:

Metric Category	Administrative Visibility Details
Number of Accounts	Admins can see the total number of active, provisioned, and suspended Gemini licenses at the University.
Usage & Prompt Metrics	Administrators within the Office of Information Technology can view metrics on a per-user basis for the number of prompts that are executed in specific apps (e.g., Gmail, Docs, Sheets, Slides, or the Gemini app) excluding Gemini Notebook, but they cannot see the content or generated response of any user interaction. They can also view the total active users per month.

Data that Google collects

Like all web-based enterprise services, Google collects necessary system telemetry to maintain security, optimize performance, and deliver the service. This includes your:

- IP address
- Browser type
- Device operating system
- Timestamp data

Data is retained for 90 days

Ninety-day retention period

Prompt history and generated content from Gemini will be retained for **90 days** in your account per University Information Security recommendations. After 90 days, any history, prompts, and generated content will be cleared from Gemini. This is a global setting for all people using Gemini at the University.

Deleting chat histories

You can manage or delete your chat histories directly within the Gemini interface. Once you delete a conversation or if your account is removed from Gemini by request or leaving the University, the data is purged from Google's active systems within standard enterprise timelines (typically 30 to 180 days depending on system backups and lifecycle rules).

Find and review stored data in Gemini

You can view, manage, and export your active interaction data directly through the Gemini activity dashboard.

For a complete record of data associated with your University account, you can use Google Takeout to download your full chat history and account data archive.

Saving your chats and prompts

To keep your chats and prompts after the 90-day retention window is up, you can save your content directly in Google Drive or manually archive it.

We recommend backing up or archiving any material you want to save or use again from Gemini before it is automatically deleted per the University's data retention policy.

Saving to a Google Doc or Gmail

Select the **Share & Export** icon at the bottom of any Gemini response and select **Export to Docs**. This creates a formatted Google Doc directly inside your UMN Google Drive.

You can also select **Draft in Gmail** from the same menu to email the thread content to yourself for archival.

Manually archiving chats and prompts

For entire conversations, copying and pasting the thread into a designated Google Doc in your drive is the most reliable way to preserve ongoing responses and notes.

Exporting data before graduation or leaving the University

After graduating or otherwise leaving the University, the data retention policy still applies until your account is closed. Learn more about exporting data before you cannot access it in the Leaving the University self-help guide.

Data requests and legal subpoenas

Understand how public records laws (MGDPA requests) apply to prompt and chat data

Because the University of Minnesota is a public institution, data generated on University-managed accounts interacts with public records laws and legal frameworks as follows:

Public records laws

Data stored within your University account may be subject to the Minnesota Government Data Practices Act (MGDPA), the state equivalent of Freedom of Information Act (FOIA), and may therefore be subject to a public data request. However, certain statutory protections (such as FERPA for student records) may apply to limit certain disclosures.

Information requests and student data

For more details on information requests and student data, review the following resources:

- Board of Regents policy on Student Data
- Board of Regents policy: Student Education Records
- Office of General Council information on Private and Public Information
- One Stop Student Services: Student records privacy and access

Deleting your data

University administrators **do not keep an archive of your prompts**. If the conversation is deleted that data no longer exists in the University's possession and cannot be retrieved for a public records or legal request.

Understand how legal subpoenas apply to prompt and chat data

Because the University of Minnesota is a public institution, data generated on University-managed accounts interacts with public records laws and legal frameworks as follows:

Legal subpoenas

In the event of litigation or a formal legal investigation involving the University, **data tied to University accounts can be subject to court-ordered discovery subpoenas or legal holds**. In the event a hold is put on data in an account, it may not be deleted until the hold is released. Learn more about data holds.

Deleting your data

University administrators **do not keep an archive of your prompts**. If the conversation is deleted that data no longer exists in the University's possession and cannot be retrieved for a public records or legal request.

Guardrails and opting out

Review guardrails and safety measures

Gemini includes specialized crisis-response protocols designed to prioritize safety and provide human connection during critical moments, operating under the following framework:

- **Automated interception and "Help Is Available" module:** When Gemini's automated real-time safety guardrails detect language indicating a potential crisis related to suicide, self-harm, or violence, it stops generating standard textual responses. Instead, it surfaces a redesigned, prominent "Help is available" module. This module provides an immediate "one-touch" interface connecting the user directly to professional resources (such as crisis hotlines, text lines, and mental health websites). This interface remains visible for the rest of the conversation to encourage the user to seek help.
- **No internal reporting to University admins or faculty:** Triggering a crisis flag **does not** send an alert to University administrators, instructors, HR, or disciplinary boards. Because the Gemini at the University operates under strict enterprise privacy parameters, prompt contents are not actively monitored or "reported out" to institutional entities for disciplinary or tracking purposes. The interaction remains isolated to your private session.
- **Data limitations:** The system does not package or transmit your conversational data to outside law enforcement or third-party crisis lines upon a trigger. Gemini simply serves as a gateway to display real-world human support resources, rather than serving as an intermediary that shares your private text.

Opt out of Gemini

If you have opted in to Gemini and want to opt out, contact Technology Help.

By opting out, you will no longer be able to access the Gemini interface. You will still have access to the University's Google Workspace tools.

Protected information guidance

Use Health Information appropriately

Staff, faculty, and people within the Healthcare Component (HCC) must take additional care in handling Health Information. Health Information includes, but is not limited to, Individually Identifiable Health Information (IIHI) and Protected Health Information (PHI).

- Any Health Information used within Gemini must follow the minimum necessary guideline (only the minimum data necessary to complete the task should be used).
- Gemini may be used for Health Information in IRB-approved studies, but any use of Gemini with Health Information, and how it is used, must be outlined in the study protocol.
- Gemini is intended to be used as a research-assistance tool; it may not be used for direct diagnosis or medical treatment.
- For Gemini and other AI questions about Health Information, please contact the Health Information Privacy & Compliance Office (HIPCO) at privacy@umn.edu.
- Healthcare Component (HCC) users must handle Health Information (including Protected Health Information) with extreme care. Gemini's use with Health Information in IRB-approved studies must be explicitly outlined in the study protocol. When using Gemini, adhere to the Minimum Necessary rule, using only the data required to complete a task. Remember, Gemini is solely a research-assistance tool and should not be used for direct diagnosis or medical treatment.

Use student information appropriately

Staff and faculty must take additional care with student information, most of which is protected by the Family Educational Rights and Privacy Act (FERPA). Because Gemini is a licensed tool, it is permissible to use with FERPA-protected data. This only applies when logged in with your University of Minnesota account in Gemini.

Only the minimum necessary information should be entered into Gemini. For example, if personally identifiable information (PII) for a student—such as their name or student ID number—is not required for the task, omit that information.

Work products created using Gemini that contain FERPA-protected information can only be shared with school officials who have a legitimate educational interest in the information.

For more information on FERPA, review the FERPA resources or take the FERPA training (SR0071). For FERPA questions, contact FERPA@umn.edu.