501CISO

501C CYBERSECURITY LEADERSHIP

Powered by ClearTone Consulting, LLC

Protecting Organizational Data

How to prevent AI Tools from Training on Your Content

Prepared by

Brian Scott

PROTECTING ORGANISATIONAL DATA

As artificial intelligence tools like ChatGPT, Google Gemini, and Microsoft Copilot become more integrated into daily operations, it is vital to ensure your organization's sensitive data and user interactions are not inadvertently used to train external AI models. This brief outlines where, how, and why you should verify your users' AI configurations, along with step-by-step guidance for top AI tools.

Why This Matters

AI tools often collect user interactions to improve performance and train future models. While this may enhance general capabilities, it can pose serious privacy, compliance, and intellectual property risks if organizational data is included.

Properly disabling data sharing for training purposes:

- Reduces risk of data leakage.
- Supports compliance with data protection laws (e.g., GDPR, HIPAA).
- Ensures intellectual property and confidential processes stay internal.

Key Platforms and How to Opt Out

1. OpenAI ChatGPT (Free & Paid Versions)

Default: Data **is** used for training unless history is disabled.

How to disable training:

1. Log in at chat.openai.com.
2. Click your **name or profile icon** → **Settings**.
3. Navigate to **Data Controls**.
4. Toggle **Chat History & Training** to **off**.

This stops conversations from being stored or used for training.

2. Google Gemini (Formerly Bard)

Default: Interactions **are** used for training.

How to disable training:

1. Go to Google Activity Controls.
2. Scroll to **Web & App Activity**.
3. Click **Manage Activity**.
4. Find **Gemini Apps Activity**.
5. Disable it to prevent data from being used to train models.

3. Microsoft Copilot (Microsoft 365 Business)

Default: Organizational content is not used to train foundation models.

What to know:

- Microsoft explicitly states that business tenant data is not used for model training.
- However, users of consumer Copilot tools (e.g., Bing or mobile apps) should check their settings individually.

How to disable consumer Copilot training:

1. Go to copilot.microsoft.com or open the Copilot mobile app.
2. Click your **profile icon** → **Settings** or **Privacy**.
3. Toggle off **Model training on text** and **Model training on voice**.

4. Anthropic Claude

Default: Data may be used to improve services unless opted out.

How to disable training:

1. Visit the Claude web app.
2. Go to **Settings**.
3. Locate data use options and disable any training-related data collection. (Note: Feature availability may vary by subscription.)

5. Perplexity AI

Default: User queries may be logged for service improvement.

How to disable training:

1. Visit perplexity.ai.
2. Click on your **profile icon** → **Settings**.
3. Toggle off usage data collection under privacy preferences.

Recommendations for Organizations

- **Issue internal guidance** to all staff using generative AI tools.
- **Restrict use of consumer AI accounts** on company devices or networks.
- **Leverage enterprise licenses** where possible, as these offer clearer data guarantees.
- **Educate employees** on the importance of protecting sensitive data when using AI.

By proactively managing AI privacy settings, organizations can maintain control over their data, protect sensitive processes, and still benefit from generative AI's capabilities.

This brief is provided by ClearTone Consulting / 501CISO, helping organizations protect their digital assets in an evolving AI-powered world. For more information, email info@501ciso.com.

501CISO
501C CYBERSECURITY LEADERSHIP
Powered by ClearTone Consulting, LLC