



GENERATIVE ARTIFICIAL INTELLIGENCE (AI) USAGE DIRECTIVES

April 1, 2026

The National Association of Pastoral Musicians (NPM) recognizes that generative AI is a rapidly developing technology that is becoming increasingly accessible to organizations of all sizes. These tools can be used to generate text, images, code snippets, and other assets, and they have the potential to revolutionize the way we work.

However, generative AI also raises a number of ethical and legal concerns. For example, there is a risk that generative AI could be used to generate false or misleading content or to discriminate against certain groups of people.

To help ensure that generative AI is used responsibly NPM has developed these guidelines, which are designed to help NPM's employees and leadership use generative AI tools in a way that is ethical, legal, and responsible.

The guidelines cover a number of topics:

- Disclosing the use of generative AI
- Protecting proprietary information
- Using AI accounts for work purposes only
- Protecting the data of users
- Sharing useful prompts with colleagues
- Sharing tips, tricks, and uses with the community
- Identifying and sharing the limits of generative AI
- Reporting incidents
- Applying an ethical framework to AI use
- Checking for intellectual property (IP) and copyright violations

Purpose

The policy outlines general principles that employees should adopt while using generative AI tools, including the evaluation of security risks and the protection of confidential data. By following these guidelines, NPM's employees will understand how to use AI tools in a secure, responsible, and confidential manner. The guidelines can help to ensure that generative AI is used in a way that benefits the organization and the community.

Definition

The term "generative AI" in this document refers to artificial intelligence that can create new content by using patterns of existing data within its framework. Current examples include: summaries of documents; drafting emails; generating blog posts; creating content for social media; and data analysis and evaluation for submitted information. Current standalone common software for Generative AI includes ChatGPT, Claude, Microsoft Copilot, and Google Gemini. Additional Generative AI is currently included in messaging functionalities for Meta, iOS, Android, as well as increased work efficiency within professional software (e.g. Microsoft Teams, Slack, Zoom).

Scope

This policy applies to all employees, contractors, and any authorized third parties who have access to or use AI tools provided or approved by NPM. This includes those who use email addresses housed within the *npm.org* domain.

Current Usage

As of April 2026, NPM's staff currently uses Generative AI for the following within the context of the Association:

- Summaries of internal meetings via its messenger service (Slack) and virtual meeting software (Zoom)
- Drafts of social media posts for initial brainstorming
- Marketing and communications campaign strategy framework
- Graphic design template suggestions via NPM's graphic design software (Canva)

Guiding Principles

These principles should guide the way employees and other relevant parties use generative AI for work. We will edit and add to these principles as we get questions, the technology changes, or new needs arise. Changes will be noted in the change log at the top of this document.

Principle 1: Disclose use of generative AI

NPM will disclose its use of generative AI in all communications, including in its privacy policy and terms of service. This will help to ensure that users know NPM is using generative AI and that they can make informed decisions about whether or not to use NPM's services.

Principle 2: Do not share proprietary information

NPM does not share proprietary information about its projects or products with generative AI tools. This includes information that is confidential, a trade secret, or otherwise protected by law.

Principle 3: Use AI accounts for work purposes only

NPM employees use their AI accounts for work purposes only. This means that they should not use their accounts for personal or private purposes. This will help to ensure that NPM's AI accounts are used for legitimate business purposes and that they are not used to violate the privacy of others.

Additionally, NPM's employees must not give access to AI tools to those outside the company without prior approval from the appropriate department or manager and without following subsequent processes required to meet security compliance requirements. This includes sharing login credentials or other sensitive information with third parties.

Principle 4: Protect the data of users

NPM protects the data of its users, including members, staff, board, volunteers, and contractors. This means that NPM will not collect or use personally identifiable information about users without their consent. NPM should also take steps to secure the data of users from unauthorized access, use, or disclosure.

Principle 5: Share useful prompts with colleagues

NPM employees can share useful prompts with their colleagues across the organization. This will help to ensure that everyone is aware of the best ways to use generative AI tools and that they are able to collaborate on projects and ideas.

Principle 6: Share tips, tricks, and uses with the community

NPM can choose to share tips, tricks, and uses for generative AI tools with the community at large. This will help to promote the responsible use of generative AI and educate others about the potential benefits and risks of this technology.

Principle 7: Identify and share the limits of generative AI

NPM will identify and share the limits of generative AI with its colleagues and the community. This includes the fact that generative AI tools are not perfect and that they can sometimes produce inaccurate or biased results. It is important to be aware of these limitations in order to use generative AI tools responsibly.

Principle 8: Check for intellectual property and copyright violations

NPM's employees and other NPM leadership should check the content produced by generative AI tools for any potential violations of intellectual property or copyright law. This includes checking for content that is copied from other sources or that uses trademarked or copyrighted images or text.

Principle 9: Report incidents

NPM's employees will log and report any incidents of AI tools malfunctioning or generating inaccurate, biased, or copyrighted information. Suspected or confirmed security incidents related to generative AI usage should be reported promptly to the organization's designated cybersecurity team or incident response personnel. Employees may also report incidents to the generative AI developers to help them identify and fix issues, as appropriate.

Principle 10: Apply an ethical framework

NPM's employees and other NPM leadership must ensure that the development, deployment, and use of AI systems meets the seven key requirements for trustworthy AI: (1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, nondiscrimination, and fairness, (6) environmental and societal well-being, and (7) accountability.

NPM's employees and other leadership should acknowledge that, while bringing substantial benefits to individuals and society, generative AI systems also pose certain risks and may have a negative impact, including impacts that may be difficult to anticipate, identify, or measure, and adopt adequate measures to reduce these risks where possible.

AI Utilization Guidelines

Each generative AI tool is unique, and use should be adapted according to the specific tool employees are using and the context in which they are using it. Being an informed and critical user of AI tools will empower employees to make better decisions and effectively leverage the technology to your advantage.

Here are a few general guidelines employees should adopt while using generative AI:

- Employees must evaluate the security of any AI tool before using it. This includes reviewing the tool's security features, terms of service, and privacy policy. Employees must also check the reputation of the tool developer and any third-party services used by the tool. The use of any new AI tools must be approved by NPM's Executive Director.
- Share tools you do not recommend that NPM use: If you are using a tool that provides bad results or discover security vulnerabilities or other concerns, please email npmsing@npm.org.

Compliance

All employees, members of the Board of Directors, and other volunteer leadership must read and agree to this policy before using any AI technologies. Failure to comply with this policy may result in disciplinary action, up to and including termination from their role within the organization.

Policy Review

This policy will be reviewed periodically to ensure its effectiveness, relevance, and compliance with changing needs, best practices, and legal requirements.

Recommendations for usage, updates, or improvements can be submitted to the Executive Director at director@npm.org.

Sources:

Language adapted with permission from Microsoft and Tech Soup's recommendation for AI Usage Policies, copyright 2023. The NPM generative AI directive is subject to change at any time. This document is the property of the National Association of Pastoral Musicians and is protected by United States and international copyright laws. For information about the directive please contact us.