RESTRICTED 2

Acceptable Usage Policy – Annex 1 – Public AI Tools

Last review date: 2025-05-15	Reviewer: Patrick Blanc, Levina Wong, Titus Halaczek
Status: Approved	Owner: Patrick Blanc

Table of Contents

1. Purpose

This annex sets forth more specific guidance under the Acceptable Usage Policy regarding the use of publicly available online Artificial Intelligence (AI) tools. It outlines the conditions under which such tools may be used for professional purposes, while ensuring that Nexthink's security, privacy, and confidentiality obligations are upheld.

2. Scope

This annex applies to all Nexthink employees subject to the Acceptable Usage Policy.

It concerns the use of external AI tools that are **publicly accessible that have not been formally reviewed or approved by Nexthink's Security, Legal, Privacy, or IT teams and for which Nexthink has not procured an enterprise-wide license**. This includes but is not limited to individual uses of: ChatGPT, Gemini, Claude, Copilot, Midjourney, and similar platforms.

Internal or vendor-hosted AI solutions formally approved by Nexthink are not subject to this annex.

3. Permitted Use

The use of external AI tools is permitted under the following conditions:

- The tool is used **exclusively for general, non-sensitive professional tasks**, such as summarizing public content, language refinement, generic code generation, or idea generation.
- Users ensure **no restricted information** is entered or shared with the AI tool (see Section 4).

This exception does not apply where the AI tool is integrated into third-party systems licensed by Nexthink. Those remain subject to Third Party Assessment process described on the Employee Portal.

4. Prohibited Data Input

The following categories of information must **never** be entered into external AI tools under this exception. Doing so may expose Nexthink to confidentiality breaches, legal liability, or regulatory non-compliance.

• Customer Data

All information received from or generated on behalf of Nexthink customers, regardless of format or context.

Examples include:

- Any text, metrics, logs, or screenshots taken from a customer environment
- Outputs from Nexthink dashboards or investigations performed for a customer
- Customer-specific configurations, user IDs, or ticket history
- Comments, complaints, or feedback received from a customer
- Customer data from a CRM tool

• Confidential Information

Information that is non-public and strategically or commercially sensitive.

Examples include:

- Internal presentations or documentation marked "Confidential" or "Restricted"
- Product roadmap details not publicly announced
- Source code or scripts written for Nexthink products
- Budget forecasts, revenue or cost figures not disclosed externally
- Meeting notes discussing business strategy, M&A, or internal challenges

• Personal Data

Any information relating to an identified or identifiable individual, whether employee, customer, candidate, or partner.

Examples include:

- Employee names, email addresses, job titles, or office locations
- CVs or candidate assessments
- Employee feedback or performance review content
- Customer support interactions or behavioral telemetry tied to a user
- IP addresses, device IDs, or session logs linked to an individual

5. Prohibited Public AI Tool

While the use of publicly available AI tools is generally permitted under this annex, certain tools are explicitly prohibited due to security, legal, or compliance concerns. Employees must not use the following tools under any circumstances when processing Nexthink-related information:

- DeepSeek
- Baidu ERNIE Bot
- YandexGPT
- Midjourney

This list is available on the Employee Portal and may be updated from time to time. Employees are responsible for ensuring they consult the most recent version before using any AI tool.

6. Practical Guidance

To help users identify restricted information:

- look for labels such as “Confidential,” “Restricted,” or “Internal Use;”
- do not use any data pulled from customer environments, support systems, or internal analytics;
- do not include names, contact details, IP addresses, access credentials, or telemetry; and
- avoid referencing unreleased product features, pricing models, legal positions, or performance metrics.

Nexthink employees are encouraged to consult the **Confidentiality Policy, AI Policy** and **Privacy Standard** when in doubt.

7. Account Ownership

Any account created or used to access publicly available AI tools for the purpose of processing or generating content on behalf of Nexthink is considered a professional account and the property of Nexthink.

Such accounts:

- must not be used for any **personal** or non-Nexthink-related activity;
- must be created using a **Nexthink email address** or identity, unless otherwise approved by the IT or Security team; and
- are subject to Nexthink's monitoring and acceptable use policies.

Upon request by Nexthink—particularly in the context of role changes, internal audits, security investigations, or offboarding—the account credentials must be:

- **handed over** to the relevant department (e.g., IT, Security, Legal), or
- **permanently deleted**, where appropriate and if requested by Nexthink.

Failure to comply with these requirements may lead to disciplinary action, in line with Nexthink's internal procedures.

8. Responsibility for AI Output

Nexthink encourages the responsible use of AI tools to foster innovation and efficiency. However, employees must understand that such tools are intended as support aids and not as substitutes for professional judgment. Employees remain fully responsible for any use of AI-generated output and are required to critically review it for accuracy, relevance, and appropriateness before applying or sharing it.

9. Accountability and Incident Management

All users are accountable for ensuring the compliant use of AI tools under this annex. Any suspected or actual breach, including the inadvertent sharing of restricted information, must be reported immediately to the **Security** and **Privacy** teams via Nexthink’s standard incident reporting process.

Improper use of AI tools may lead to **disciplinary action**, in accordance with Nexthink’s internal procedures.

10. Governance

This annex forms an integral part of the Acceptable Usage Policy. It may be updated independently to reflect evolving technology, regulatory requirements, or business risk assessments. The most recent version will be maintained in the central policy repository.