PxNDA

Acceptable Use Policy

Boundaries of lawful and ethical use of PxNDA.

Effective May 16, 2026 · Version 1.0

↓ Download PDF

1. Purpose & Philosophy

PxNDA is built to protect legitimate confidentiality — the kind that enables creative collaboration, business partnerships, and the secure exchange of sensitive information between willing, informed parties.

PxNDA is not, and will never be, a tool for suppressing truth, silencing victims, enabling abuse, or circumventing justice.

This Acceptable Use Policy ("AUP") defines the boundaries of lawful and ethical use of the PxNDA platform. Violation of this policy results in immediate account termination, voiding of affected agreements, and where appropriate, reporting to law enforcement.

⚠ **ABSOLUTE PROHIBITIONS — These uses are void, unenforceable, and grounds for immediate termination:**

- Using NDAs to silence, intimidate, or coerce victims of harassment, sexual abuse, or assault
- Using NDAs to conceal criminal activity or protect perpetrators of crimes
- Using NDAs to suppress whistleblowing or reporting of illegal conduct
- Using NDAs to prevent users from cooperating with law enforcement or regulatory authorities
- Any use that violates applicable law, human rights, or fundamental freedoms

2. The NDA Abuse Problem — Our Stance

Non-Disclosure Agreements have been weaponized by powerful individuals and institutions to silence victims of abuse, harassment, and misconduct. High-profile cases globally have demonstrated how NDAs can be used to:

- Prevent victims of sexual harassment or assault from speaking to journalists, law enforcement, or support networks
- Protect serial abusers from accountability by legally threatening victims into silence
- Create psychological coercion — making victims believe they cannot seek help without legal consequences
- Obstruct justice by prohibiting cooperation with investigations

PxNDA categorically rejects this misuse. NDAs generated and executed through PxNDA are for legitimate business and creative confidentiality only.

3. What Makes an NDA Void & Unenforceable on PxNDA

The following types of NDAs are void and unenforceable regardless of whether they are signed through PxNDA:

3.1 Abuse & Harassment Silencing NDAs

> **VOID BY LAW AND BY POLICY:**
>
> - Any NDA that attempts to prevent disclosure of sexual harassment, sexual assault, or domestic violence
> - Any NDA that conditions employment, compensation, or benefits on waiving the right to report abuse
> - Any NDA designed to protect an abuser from consequences of their own misconduct
> - Any NDA that prohibits a victim from seeking medical, psychological, or legal help
> - Any NDA that prevents a person from naming their abuser to law enforcement or courts

Legal basis: In the United States, the Speak Out Act (2022) and VAWA (Violence Against Women Act) restrict enforceability of NDAs in sexual misconduct cases. In the EU, the EU Pay Transparency Directive and member state laws protect workers' rights to report abuse. In the Dominican Republic, Ley 24-97 (violence against women) and constitutional protections override any contractual silencing attempt.

3.2 Criminal Activity Concealment NDAs

- NDAs cannot be used to conceal ongoing or past criminal activity
- NDAs cannot prevent reporting of suspected child abuse, elder abuse, or human trafficking
- NDAs cannot prohibit cooperation with law enforcement investigations
- NDAs cannot protect parties who have committed fraud, embezzlement, or financial crimes
- Any NDA with a purpose that requires concealing illegal conduct is void **ab initio** (void from the beginning)

3.3 Whistleblower Suppression NDAs

- NDAs cannot prevent reporting of regulatory violations to government agencies
- NDAs cannot prohibit disclosures protected under whistleblower protection laws
- NDAs cannot prevent reporting to the SEC, OSHA, NLRB, or equivalent regulatory bodies
- In the EU, the EU Whistleblower Directive (2019/1937) establishes non-waivable protections

3.4 Public Safety Threat NDAs

- NDAs cannot prevent disclosure of imminent threats to public health or safety
- NDAs cannot prohibit reporting of product defects that endanger consumers
- NDAs cannot silence reporting of environmental hazards or contamination

4. Permitted Uses of PxNDA

PxNDA is designed for legitimate confidentiality in the following contexts:

- **Business partnerships:** protecting trade secrets, product roadmaps, financial projections
- **Creative collaboration:** protecting unreleased music, film, design, and creative works
- **Employment:** protecting proprietary information during recruitment or onboarding
- **Legal and financial:** protecting privileged information during due diligence or negotiations
- **Technology:** protecting source code, technical specifications, and architectural designs
- **Media and entertainment:** protecting scripts, unannounced projects, and production details

5. AI-Generated NDA Responsibility

PxNDA uses artificial intelligence (Anthropic's Claude API) to generate NDA clauses. Users are exclusively responsible for:

- Reviewing all AI-generated content before signing or sending
- Ensuring the NDA does not include prohibited clauses as defined in Section 3
- Confirming the NDA complies with applicable law in all relevant jurisdictions
- Obtaining legal counsel for high-stakes agreements

PxNDA's AI is designed to generate standard business confidentiality clauses. It is NOT designed to generate clauses that would silence victims, conceal crimes, or suppress protected disclosures. If the AI generates content that appears to violate this policy, do not use it and report it to pxnda@algomejor.do.

PxNDA is not a law firm. AI-generated NDAs are drafts and are not legal advice. PxNDA assumes no liability for the legal validity, enforceability, or consequences of agreements executed through the platform.

6. File Transfer Content Policy

Files transferred through PxNDA must not contain:

- **Child sexual abuse material (CSAM)** — zero tolerance, reported to NCMEC and law enforcement
- Content that facilitates violence, terrorism, or human trafficking
- Malware, ransomware, or malicious code
- Stolen intellectual property or trade secrets obtained through illegal means
- Non-consensual intimate images (NCII)
- Any content that violates applicable law

We reserve the right to review flagged content and cooperate with law enforcement investigations.

7. Enforcement

7.1 Reporting Violations

If you believe an agreement on PxNDA violates this policy — particularly if you have received an NDA that appears designed to silence you — please contact us immediately:

> Email: pxnda@algomejor.do
> Subject: "AUP Violation Report"

We take all reports seriously. If you are a victim who has received a potentially coercive NDA through PxNDA, we will **not enforce** that agreement and will assist you in understanding your rights.

7.2 Consequences of Violations

- Immediate account suspension or termination
- Voiding of the affected agreement(s)
- Preservation and disclosure of records to law enforcement upon lawful request
- Civil liability for damages caused to affected parties
- Reporting to relevant authorities where required by law

7.3 Safe Harbor for Victims

> If you signed a PxNDA agreement under duress, coercion, or as a condition of receiving something you were entitled to (employment, payment, safety), **that agreement may be unenforceable**. PxNDA will not take any action to enforce agreements that violate this policy or applicable law. We encourage you to seek legal counsel.

8. Governing Law & Jurisdiction

This AUP is governed by the laws of the Dominican Republic and applicable international law. For users in the EU, mandatory EU consumer and human rights protections apply regardless of any choice of law clause.

The prohibitions in Section 3 apply **regardless of the law chosen by the parties** in any NDA, as they reflect mandatory public policy rules that cannot be contracted away.

9. Contact

Algo Mejor Media Labs — PxNDA

Email: pxnda@algomejor.do

Website: pxnda.com

Location: Santo Domingo, Dominican Republic