

Confidentiality, Privacy, and Team Code of Conduct Agreement

Concise Reading Version • Version 0.1 • Draft Date: September 1, 2026

Important: This document is provided for online reading and acknowledgment. It is not a form to download, print, fill out, or sign. The source agreement is a draft requiring legal review. Its substantive terms should remain subject to that review.

Six Simple Promises

- Protect people: never reveal who a protected story is about.
- Protect FANOS: keep plans, products, services, finances, partnerships, and internal work private.
- Use information only for assigned FANOS work.
- Use only approved accounts, folders, devices, and tools.
- Report mistakes or concerns right away; hiding a problem creates more risk.
- Treat every person with dignity, respect, honesty, and care.

1. Purpose and Who This Agreement Covers

This Agreement is between FANOS Enterprises, LLC ("FANOS") and the person who receives access to FANOS information ("Team Member"). It protects people whose lives or experiences are discussed through Alchemizing Stories; team members; guests, applicants, clients, vendors, and partners; FANOS business information; and FANOS services, products, tools, offerings, and future plans.

It applies to employees, contractors, interns, student mentees, volunteers, advisors, and anyone else who receives FANOS information, whether written, spoken, photographed, recorded, electronic, seen in a meeting, or learned informally.

2. What Counts as Confidential Information

Protected Story and Personal Information

- Protected identities, pseudonym keys, names, initials, faces, voices, handwriting, photos, usernames, contact information, exact locations, dates, ages, jobs, family relationships, immigration, religious-community, employment, financial, medical, mental-health, disability, legal, and family information.
- Identities of institutions discussed in protected stories, plus raw footage/audio, transcripts, notes, messages, records, screenshots, drafts, captions, comments, file names, tags, version histories, links, metadata, and combinations of details that could identify a person or institution.

FANOS Proprietary Business Information

- Business/strategic plans, roadmaps, priorities, planned services/products/programs/workshops/consultations, unpublished tools, libraries, applications, technology ideas, prototypes, frameworks, methods, processes, research, literary/family-story projects, pricing, budgets, expenses, revenue, forecasts, funding/grants, financial/tax/insurance records, contracts, legal advice, negotiations, staffing, compensation, and internal decisions.
- Unpublished episodes, scripts, research, editorial calendars, production plans, audience/analytics/marketing/growth information, vendor/sponsor/client/partner lists, outreach/collaboration plans, developing brand assets, trademarks/logos/taglines/designs/templates, SOPs/playbooks/trackers/dashboards/project plans, account lists/workflows, and other non-public information that could enable copying, competition, interference, or exploitation.

Security and Third-Party Information

- Passwords, recovery codes, account numbers, access links, security questions/authentication information, API keys, device information, FANOS security information, and confidential information received from clients, guests, team members, applicants, vendors, partners, attorneys, accountants, or other third parties.

3. Strict Story-Privacy Rule: No Personal Identifiers

Non-negotiable: Do not share, publish, discuss, confirm, deny, hint at, or help another person identify any protected person or institution connected to an Alchemizing Stories narrative.

This applies in public and private settings, including family/friends, school assignments, group chats, texts/private messages, social media, portfolios, resumes, scholarship/school/job applications, personal projects, other employment, and work for another organization.

- Use only FANOS-approved pseudonyms and general/published descriptions.
- Remove identifying details from drafts, file names, comments, captions, thumbnails, tags, prompts, version histories, and metadata.
- Never keep a pseudonym-to-real-identity list without Founder/legal-counsel approval.
- Never confirm/deny guesses or connect a FANOS story to information found elsewhere.
- Avoid exact dates, locations, ages, positions, and unusual facts that could identify someone.
- Stop and ask before using a detail that could identify someone when combined with other information.

Public Guests and Contributors

A guest may be named, photographed, recorded, or shown only when FANOS confirms authorization for that specific public use. Authorization is limited to the approved guest, content, platform, purpose, and period. It does not permit revealing another anonymous person/institution, sharing unpublished recordings/conversations, using the material in a personal portfolio, or sharing it outside the approved FANOS publication.

4. How Confidential Information May Be Used

Use Confidential Information only when **all three** are true: (1) it is needed for a specific FANOS assignment; (2) you have access or written approval; and (3) it is handled through an approved FANOS process/system. Access depends on need, role, and approval—not simply team membership.

- No personal gain, school credit without written approval, another business/organization/competing project, or separate product/service/organization/commercial opportunity.
- No copying, photographing, screen-recording, screenshots, downloading, printing, forwarding, or removing without approval/assignment need.
- No giving information to a team member without need, or contacting protected story subjects without authorization.
- No contacting applicants, clients, vendors, partners, institutions, or media unless specifically assigned and authorized.

5. Technology, Account, and File Security

- Use individual accounts unless instructed otherwise; strong passwords; and multi-factor authentication when available.
- Use only FANOS-approved folders/accounts/devices/sharing settings; share only with specifically named people who need access; check permissions before links are sent/published.
- Lock devices, keep software/security updates reasonably current, protect screens/documents, and immediately report suspicious logins, exposed passwords, or lost devices.
- Do not send passwords/recovery codes through ordinary email, text, chat, Google Docs, GitHub, or shared documents except approved exceptions; do not store them in ordinary spreadsheets/documents except approved exceptions.
- Do not use “anyone with the link” unless approved; move FANOS files to personal email/cloud/camera roll/USB/unapproved apps; use shared/public computers for sensitive information without approval; leave confidential information visible; or delete official FANOS records without approval.
- Keep passwords, recovery codes, and other sensitive access information in a secure password manager.

Personal Devices

An approved personal device must have a passcode/password, current security updates, automatic screen locking, and reasonable privacy protections. Approved temporary downloads must be deleted from downloads, desktop, camera roll, trash/recycle folders, personal cloud backups, and other personal storage after the official FANOS copy is uploaded and confirmed. Do not delete the official copy.

6. Artificial Intelligence: Ask Before Uploading

Without written approval, do not put Confidential Information, financial records, legal documents, partner/vendor information, or identifying story details into public/personal AI tools, transcription/translation services, editing/design platforms, storage platforms, or other outside services.

- Never enter real names or other personal identifiers into AI prompts.
- Use the minimum information needed and de-identify it first.

- Review sharing/retention settings when instructed.
- Verify facts, citations, translations, and quotations.
- Have a human review every output before FANOS uses or publishes it.
- Do not present AI-generated material as verified human knowledge without appropriate review.

7. Publishing, Public Statements, Portfolios, and Social Media

Only the Founder, CEO, or another person designated in writing may give final approval to publish, release, or share FANOS content.

- Silence is not approval; a complete-looking draft is not automatically approved.
- Publish approved material exactly as approved; substantive changes require new approval.
- Do not change titles, names, facts, images, captions, links, or claims without authorization.
- Do not speak publicly for FANOS, respond to reporters/media, or make legal, medical, tax, or financial claims for FANOS without authorization.
- Do not promise products, payment, partnerships, services, or benefits without authorization.
- Do not post confidential behind-the-scenes information on personal accounts.

Do not publicly share internal screenshots, private meetings/conversations, unfinished documents, internal disagreements, confidential accomplishments, unreleased logos/products, team messages, private photos, confidential schedules, or protected-story information. Do not use FANOS documents, screenshots, data, recordings, plans, work samples, or internal tools in portfolios, class assignments, school competitions, academic/job/scholarship applications, or personal projects without prior written approval and complete de-identification.

8. Team Code of Conduct

Dignity, Care, and Trauma-Informed Behavior

- Treat each person as a human being—not content, a diagnosis, a mistake, or an attention opportunity.
- Protect dignity and the meaning of experiences; use respectful, accessible language.
- Avoid judgmental/humiliating language and pressure to share more than someone wishes.
- Access to someone's story is a responsibility, not an entitlement.
- Do not gossip, shame, blame, sensationalize, mock, exploit, manipulate, pressure, or use another person's pain for attention/personal gain.

Respectful and Safe Workplace

FANOS does not permit discrimination, harassment, sexual harassment, bullying, threats, intimidation, retaliation, degrading conduct, coercion, or unwanted sexual/romantic conduct. Respect differences in race, color, national origin, ethnicity, culture, language, religion/faith, sex, pregnancy, disability, age, sexual orientation, gender identity, family status, immigration background, health status, and experience/authority. Report unsafe, coercive, discriminatory, harassing, retaliatory, or inappropriate conduct. No one will be punished for a good-faith report, asking for help, or truthful participation in a review.

Accuracy and Integrity

- Do not invent/misrepresent facts, citations, quotations, credentials, partnerships, results, audience numbers, research findings, or project status.
- Do not plagiarize, misleadingly alter quotations, manipulate stories, present assumptions as verified facts, hide errors, falsely claim AI statements are verified, or claim another person's work as your own.
- Correct mistakes promptly; distinguish facts from ideas/assumptions; identify sources when appropriate; preserve speakers' intended meaning; tell the Founder when unsure.

Professional Boundaries and Conflicts

Do not privately solicit money, gifts, favors, business, romantic attention, personal services, employment, private health/financial information, or another personal benefit from story subjects, applicants, audience members, vendors, or partners. Disclose personal, family, financial, school, employment, or business relationships that could affect impartiality, influence decisions, create divided loyalty, or appear to create a conflict. Do not accept gifts, discounts, free products, referral payments, or special benefits connected to FANOS work without written approval.

Student and Minor Safety

- Student interns receive only the minimum information/access needed for age-appropriate assignments.
- No one may instruct a student to hide work-related contact, messages, meetings, assignments, safety/privacy concerns, uncomfortable conduct, or incidents from a parent/guardian, FANOS leadership, counsel, or another trusted adult.
- Students may ask questions, request clearer instructions, seek adult review, report discomfort, identify overly advanced tasks, decline unsafe/unapproved tasks, and request a parent/guardian/trusted adult, without retaliation.
- Student communications/meetings/deadlines should use approved channels, reasonable hours, clear supervision, age-appropriate tasks, and role-based access limits.

9. What to Do If Something Goes Wrong

Report it immediately—even if you are unsure whether harm occurred. Report lost/stolen devices, wrong-recipient messages, incorrect sharing settings, suspicious logins, missing files, exposed passwords, accidental publication, identifying story details, wrong-folder placement, unauthorized downloads, inappropriate conduct, harassment/retaliation, requests to hide information, conflicts of interest, and other privacy/security/conduct problems.

Use FANOS's designated reporting channel or the alternate contact/counsel process when the concern involves the normal recipient. When reporting, explain what happened, when, what information/account may be involved, who may have received/seen it, what device/system was involved, and immediate steps taken.

- Do not hide the problem, destroy evidence, alter records to cover a mistake, contact affected people without instructions, contact media, make public statements, or independently investigate another person.
- FANOS determines appropriate next steps.
- Promptly reported good-faith mistakes are handled differently from intentional misuse, concealment, retaliation, or repeated disregard.

10. FANOS Responsibilities

- Provide understandable, age-appropriate confidentiality instructions and explain role/authority.
- Provide approved work systems and limit access to the minimum reasonably needed.
- Protect Team Member personal information and avoid public sharing without permission, except as required/permitted by law.
- Provide reporting channels for privacy, conduct, safety, harassment, discrimination, and retaliation concerns.
- Respond to good-faith reports without retaliation and take reasonable corrective action when needed.
- Provide appropriate supervision for student Team Members.

11. Return, Deletion, and End of Access

- Return FANOS property/materials; stop using FANOS accounts, systems, and Confidential Information.
- Return keys, equipment, records, and FANOS-owned devices.
- Delete approved temporary copies and remove FANOS information from personal email/cloud, downloads, trash, backups, and other personal locations.
- Help transfer unfinished work/records and provide necessary account/project-status information.
- Confirm completion in writing if requested.
- Do not delete or alter official FANOS records; FANOS decides what must be preserved.

12. How Long the Duties Last

Duties begin when the Team Member first receives Confidential Information and continue throughout the FANOS relationship and after it ends. Protected story information, personal information, passwords/credentials, security information, third-party confidential information, and trade secrets remain protected as long as they remain private or protected by law. Other proprietary business information remains protected until FANOS authorizes release or it becomes public without a violation.

13. Information Not Covered

Confidential Information does not include information the Team Member can prove became public through authorized release or without breach; was lawfully known before disclosure; was lawfully received from someone entitled to disclose it; or was independently developed without using FANOS Confidential Information.

Protected-story special rule: Even if public information could identify a person/institution, the Team Member may not confirm, deny, connect, or discuss the identity based on knowledge gained through FANOS.

14. Legally Protected Reports and Disclosures

Nothing prevents or punishes reporting suspected unlawful conduct, fraud, discrimination, harassment/sexual harassment, sexual assault, retaliation, safety concerns, or other legally protected concerns; discussing/reporting wages or working conditions when protected by law; contacting government agencies/law enforcement; consulting an attorney; speaking with a parent/guardian; responding truthfully to lawful legal process; cooperating with government investigations; participating in protected workplace investigations; or exercising another legally protected right. No FANOS permission is required for a legally protected report.

Trade Secret Immunity Notice

Under 18 U.S.C. § 1833(b), an individual may disclose a trade secret in confidence to a government official or attorney solely to report/investigate a suspected legal violation, in a sealed court document, or to an attorney concerning a retaliation claim, subject to applicable confidentiality requirements. A qualifying disclosure does not create liability under federal or state trade-secret law. This Agreement is not intended to conceal sexual harassment/sexual assault or restrict legally protected reports. When another disclosure is legally required, give FANOS prompt notice when law permits so FANOS can seek appropriate protection.

15. Limited Permission and No Transfer of Rights

FANOS grants only the limited permission needed for approved work. No other license, ownership interest, or permission is granted. Access to FANOS documents, ideas, files, accounts, or tools does not mean ownership or permission to use them elsewhere. Ownership of FANOS-created work, pre-existing materials, inventions, content, designs, photos, recordings, code, research products, and other intellectual property should be addressed in the applicable employment, contractor, internship, volunteer, contributor, or other role agreement.

16. Consequences and Lawful Remedies

A violation may result in access suspension, assignment removal, corrective action, additional training, discipline, termination of the FANOS relationship, required return/deletion, or another lawful response. FANOS may seek court orders stopping use/disclosure, return/destruction of unauthorized copies, compensation for legally recognized harm, and other remedies available by contract or law. Promptly reported good-faith mistakes are treated differently from intentional disclosure, personal misuse, concealment, retaliation, dishonesty, or repeated disregard of privacy/security rules.

17. General Terms

- This Agreement supplements, but does not replace, any role agreement, privacy policy, release, client obligation, or other duty providing greater protection.
- It does not promise employment, compensation, a specific assignment, or a particular length of service.
- Changes must be in writing and approved by FANOS and the Team Member.
- FANOS may issue reasonable privacy/security procedures that do not reduce legally protected rights.
- If one part is unenforceable, the rest continues to apply to the fullest extent allowed by law.
- A delay in enforcing a provision does not waive it.
- Proposed governing law and venue: Commonwealth of Virginia, unless legal counsel determines another jurisdiction should apply.
- Electronic signatures and signed counterparts may be used to the extent allowed by law.
- If the Agreement conflicts with a legally protected right, the protected right controls.

18. Online Acknowledgment

The website—not this PDF—is the place where the Team Member will complete the acknowledgment. The web workflow should present the agreement, allow the Team Member to confirm that they reviewed and understood it, and collect the required acknowledgment information electronically. No information needs to be written into or signed on this PDF.

Parent or Guardian — Online Acknowledgment When Required

Where the Team Member is under 18, the website should present the parent/guardian acknowledgment separately and collect the required guardian information electronically. The source agreement states that legal counsel should confirm the legal effect of the guardian acknowledgment in the applicable jurisdiction.

Internal FANOS Alignment — Non-Operative

This concise reading version supports existing FANOS expectations concerning confidentiality for family and health-related stories; privacy for applicants, guests, vendors, and partners; role-based access; password-manager use; multi-factor authentication; limits on team authority; human review before publishing; ethical storytelling; business continuity; and protection of FANOS products, services, plans, offerings, and intellectual property.