# Essential Nonprofit Board Policies

An explainer guide for executive directors and board members

NOAH E. SPIEGEL CONSULTING

A great board and a capable ED will take you pretty far. But governance also runs on something more concrete: written policies that actually get used — ones that protect the organization, guide real decisions, and hold up to scrutiny when funders or regulators come looking.

This guide covers five policies that every 501(c)(3) organization should have in place. For each one, you will find: what it is, why it matters, what it should address, questions to ask about your current policy, and the warning signs that yours needs attention.

**These are explainer guides, not sample policies.** Every organization's policies should be tailored to its circumstances and reviewed by legal counsel. Use this to understand what you're working toward — not as a substitute for doing that work.


| | |
|---|---|
| 01 | **Conflict of Interest Policy** |
| 02 | **Whistleblower Protection Policy** |
| 03 | **Confidentiality Policy** |
| 04 | **Document Retention and Destruction Policy** |
| 05 | **Social Media and Media Relations Policy** |



**Legal disclaimer:**
The information in this guide is intended for educational purposes only and does not constitute legal advice. Nonprofit policy requirements vary by state, organizational size, funding sources, and sector. The questions and frameworks provided here are designed to help boards and executive directors think through their policies — not to substitute for professional legal counsel. Before adopting, amending, or relying on any organizational policy, consult a qualified attorney familiar with nonprofit law in your state.


## 01 Conflict of Interest Policy

Protecting the organization’s decisions from personal financial interests

### What It Is

**A conflict of interest policy establishes the rules for identifying, disclosing, and managing situations where a board member’s, officer’s, or key employee’s personal financial interests could influence — or appear to influence — their decisions on behalf of the organization.**

**The IRS takes this seriously. Form 990 asks whether the organization has a written conflict of interest policy, whether officers and directors complete annual disclosure statements, and whether the organization regularly monitors compliance. A missing or unused policy is a red flag.**

### Why It Matters

Conflicts of interest aren't inherently wrongdoing. They're a predictable feature of governance — board members bring valuable networks and relationships, and those same connections sometimes create conflicts. The policy's job isn't to prevent conflicts from existing. It's to make sure they're disclosed, handled openly, and kept from tainting organizational decisions.

Without a functioning conflict of interest policy, organizations are exposed to:

- IRS scrutiny and potential loss of tax-exempt status in severe cases
- Private benefit transactions that violate federal tax law
- Legal liability for board members who benefit improperly from their positions
- Reputational damage if undisclosed conflicts become public
- Funder concerns — many foundations require a conflict of interest policy as a grant condition

### What It Should Address

- [ ] A clear definition of what constitutes a conflict of interest, including financial interests of immediate family members
- [ ] Which individuals are covered: board members, officers, key employees, and committee members with governance authority
- [ ] A requirement to disclose potential conflicts before they influence decisions
- [ ] The process for recusal: the conflicted individual must leave the discussion and the vote
- [ ] Annual disclosure statements — a written form signed by all covered individuals
- [ ] How disclosures are recorded in meeting minutes
- [ ] Who is responsible for monitoring compliance (typically the board chair or governance committee)
- [ ] Consequences for failure to disclose a conflict

### Questions to Ask About Your Policy

- Does every board member sign a disclosure statement at least annually?
- Are signed disclosures actually retained on file?
- Do board members know they are required to disclose and recuse — or is it assumed they already know?
- Is the recusal process followed consistently in meetings, including being documented in minutes?
- Does the policy cover family members and organizations with which board members have a financial relationship?
- When was the policy last reviewed by an attorney?

**Common gap:**
Many organizations have a conflict of interest policy but no one signs it annually, no one tracks disclosures, and no one leaves the room when a conflict arises. A policy that exists on paper but is not practiced is not a policy — it is a liability.

## 02 Whistleblower Protection Policy

Protecting people who report suspected wrongdoing in good faith

### What It Is

**A whistleblower protection policy establishes a process for board members, staff, and volunteers to report suspected illegal activity, financial misconduct, or serious violations of organizational policy — and protects those who make such reports from retaliation.**

**Federal law — specifically the Sarbanes-Oxley Act — prohibits retaliation against nonprofit employees who report suspected fraud or financial wrongdoing. Form 990 asks whether the organization has a written whistleblower policy. This is not optional for any organization that intends to operate with credibility.**

## Why It Matters

Internal misconduct is most often discovered by people inside the organization — staff, volunteers, or board members who notice something that does not look right. Without a clear, protected channel to report concerns, most people will stay silent. By the time problems surface externally, the damage is often far worse than it would have been.

A whistleblower policy tells staff that raising legitimate concerns won't cost them their job. It tells your board that accountability is built into how the organization operates — not just aspirational. And it gives funders and regulators something concrete to point to when they ask whether internal checks actually exist.

## What It Should Address

- [ ] A clear statement that retaliation against good-faith reporters is prohibited and subject to discipline
- [ ] Who may make a report: board members, staff, volunteers, and in some cases contractors
- [ ] What types of concerns the policy covers: financial fraud, theft, falsification of records, serious legal violations, and significant policy violations
- [ ] How to submit a report — and to whom, with an alternative recipient for concerns about the ED or a senior staff member
- [ ] How reports will be investigated and by whom
- [ ] Confidentiality protections for reporters, to the extent possible
- [ ] A statement that knowingly false reports made in bad faith are not protected
- [ ] The role of the board (typically the audit or finance committee, or the board chair) in receiving and overseeing serious reports

## Questions to Ask About Your Policy

- Do staff actually know this policy exists and how to use it?
- Is there a clear alternative reporting path if the concern involves the executive director?
- Who receives reports, and is that person genuinely independent of the concern being raised?
- How are reports investigated, and is that process documented?
- Has anyone ever actually used this process? If not, does that mean the culture does not support it?
- Does the policy cover board members as potential subjects of a report — not just staff?

**On culture:**
A whistleblower policy is only as strong as the culture around it. If staff fear retaliation despite written protections, the policy provides little real protection. The board should periodically ask leadership whether staff feel safe raising concerns — and should treat that question seriously.

## 03 Confidentiality Policy

Defining what board members and staff may and may not share outside the organization

### What It Is

**A confidentiality policy establishes what information board members, officers, and staff are expected to keep private, and under what circumstances information may or may not be shared outside the organization.**

**Unlike some other policies, confidentiality isn't primarily driven by a single federal law. It's a governance best practice rooted in multiple overlapping concerns: fiduciary duty, donor privacy, employment law, funder requirements, and the basic trust that makes a board function. Organizations working with vulnerable populations, sensitive client data, or competitive funding environments carry additional obligations worth taking seriously.**

### Why It Matters

Board members are regularly trusted with information that could do real damage in the wrong hands: personnel matters, financial details, donor identities, strategic plans, legal concerns, and client data. Most people understand this intuitively when they join a board. But intuition isn't a policy, and the gap between the two is where breaches happen.

- Breach of donor privacy erodes trust and may violate state charitable solicitation laws
- Personnel information shared outside proper channels creates legal exposure
- Premature disclosure of strategic plans can harm competitive positioning or funder relationships
- Client or participant data disclosed without consent may violate privacy laws, including HIPAA in healthcare-adjacent contexts
- Board members who share confidential deliberations undermine board cohesion and trust

### What It Should Address

- [ ] A definition of confidential information: personnel records, financial details not publicly disclosed, donor information, legal matters, client/participant data, and board deliberations
- [ ] Who is covered: board members, officers, key staff, volunteers with access to sensitive information
- [ ] The expectation that confidentiality continues after a board member’s term ends
- [ ] Specific guidance on donor information: names, gift amounts, and contact information are typically confidential unless donors have consented to recognition
- [ ] Client and participant data: how it may be stored, accessed, and shared (including any applicable legal requirements such as HIPAA)
- [ ] Board deliberations: the norm that what is discussed in the boardroom stays in the boardroom, separate from what is communicated publicly
- [ ] Exceptions: situations where disclosure is legally required or appropriate
- [ ] How violations are reported and addressed

### Questions to Ask About Your Policy

- Do board members receive a copy of and sign the confidentiality policy at orientation?

- Is the policy clear about what happens to confidentiality obligations when a board member's term ends?
- Does the policy specifically address social media — what board members may and may not post about board discussions?
- If the organization works with clients or participants, does it have a separate data privacy policy that aligns with this one?
- Are staff clear on what information they may share with board members and what requires executive authorization?
- When did your legal counsel last review this policy?

**On board deliberations:**
One of the most common confidentiality breaches is not malicious — it is a board member mentioning the substance of a closed board discussion to a colleague, donor, or community contact. The policy should name this explicitly and establish a shared understanding that board cohesion depends on discretion.

## 04 Document Retention and Destruction Policy

Establishing how long records are kept, how they are stored, and how they are disposed of

### What It Is

**A document retention and destruction policy specifies which organizational records must be kept, for how long, in what format, and how they should be disposed of when the retention period expires. It also establishes that destruction of documents must be suspended immediately when litigation, audit, or investigation is anticipated or underway.**

**Form 990 asks whether the organization has a written document retention policy. Sarbanes-Oxley makes it a federal crime to knowingly destroy documents relevant to a federal investigation. If you want to operate with credibility and legal cover, this policy is not optional.**

### Why It Matters

Organizations generate and accumulate enormous volumes of records — financial, legal, personnel, programmatic, and governance. Without a clear policy, organizations tend toward one of two dysfunctional extremes: keeping everything indefinitely (creating storage burden and legal risk), or deleting things haphazardly (creating legal exposure when records are needed).

A good retention policy:

- Protects the organization during audits, litigation, and regulatory inquiries
- Reduces storage costs and administrative burden by authorizing the disposal of records past their useful life
- Gives funders and oversight bodies evidence that you're managing records responsibly
- Creates shared expectations across staff and board so records are managed consistently

### What It Should Address

- [ ] A schedule specifying retention periods for major categories of records (see key categories below)
- [ ] Whether records may be kept in digital format, and if so, what standards apply to digital storage and backup

- [ ] The process for authorized destruction of records past their retention period
- [ ] A litigation hold provision: all destruction must stop immediately when legal action is threatened or reasonably anticipated
- [ ] Who is responsible for overseeing the retention schedule and authorizing destruction
- [ ] How the policy applies to electronic communications including email

### Key Record Categories and Typical Retention Periods

| Record type | Typical retention period |
|---|---|
| Corporate records (articles, bylaws, board minutes, IRS determination letter) | **Permanent** |
| Audited financial statements and audit reports | **Permanent** |
| IRS Form 990 filings | **Permanent** |
| Grant agreements and final reports | **10 years after close** |
| General financial records, ledgers, and bank statements | **7 years** |
| Contracts and legal agreements | **7 years after expiration** |
| Personnel records (current employees) | **Duration of employment + 7 years** |
| Personnel records (former employees) | **7 years after separation** |
| Payroll records and tax filings | **7 years** |
| Insurance policies | **Permanent (or 10 years after expiration)** |
| General correspondence | **3 years** |
| Routine administrative records | **3 years or when superseded** |

## Questions to Ask About Your Policy

- Does staff know this policy exists and apply it consistently?
- Who is authorized to approve document destruction — and does that actually happen, or do records just accumulate?
- Does your policy address email and digital records, or only physical files?
- Is there a clear litigation hold procedure, and does leadership know to invoke it immediately if legal action is threatened?
- When was this policy last reviewed — particularly in light of changes to your digital storage practices?

**Critical point:**
Destroying records after you have reason to believe litigation or a government inquiry is coming is a federal crime under Sarbanes-Oxley, regardless of whether your document retention policy would otherwise permit it. Every ED and board chair should know to issue an immediate hold before any routine destruction proceeds when legal trouble is on the horizon.

05

## DSocial Media and Media Relations Policy

Governing how the organization and its people communicate publicly

### What It Is

**A social media and media relations policy establishes guidelines for how the organization communicates through social media channels and with news media — including who speaks on behalf of the organization, what may and may not be shared, and how individual board members and staff should conduct themselves on personal platforms when they are identifiable as organizational representatives.**

**This is the newest of the five essential policies and the one most likely to be missing or outdated. The risks are real, and they tend to surface faster than most organizations expect.**

### Why It Matters

The lines between organizational voice and personal voice have blurred significantly. A board member tweeting their opinion of a community controversy, a staff member posting a photo from a restricted program, or an ED commenting on a political issue without authorization can all create organizational consequences — with or without intent.

Organizations without clear policies in this area face:

- Reputational damage from public statements that do not reflect organizational positions
- Confidentiality breaches when internal information, client images, or program details are shared publicly
- Political activity concerns if individuals appear to speak for the organization on partisan issues (a 501(c)(3) compliance risk)
- Crisis communications problems when multiple people respond to media inquiries with inconsistent messages
- Employment and HR issues when staff social media activity creates a hostile environment or harms the organization

### What It Should Address

#### Organizational social media accounts

- [ ] Who is authorized to post on behalf of the organization on official channels
- [ ] Approval process for content, especially on sensitive topics
- [ ] Brand standards: tone, visual identity, messaging consistency
- [ ] How to respond to critical or negative comments, and who is authorized to do so
- [ ] What to do in a social media crisis: escalation path and who holds the account credentials
- [ ] Restrictions on political content that could jeopardize 501(c)(3) status

#### Staff and board personal social media

- [ ] A clear statement that employees and board members are personally responsible for their personal social media activity
- [ ] Guidance on identifying oneself as affiliated with the organization and what that implies
- [ ] Expectations around confidentiality: not sharing client images, program details, internal conflicts, or board deliberations
- [ ] Guidance on political activity: individuals may express personal views, but not in ways that appear to represent the organization
- [ ] Expectations around professional conduct: harassment, discrimination, or content that would embarrass the organization

### Media Relations

- ☐ Designation of an official organizational spokesperson (typically the ED, with the board chair as backup)
- ☐ Instruction that all media inquiries should be directed to the designated spokesperson before any response is given
- ☐ Guidelines for what may be shared with media and what requires board authorization
- ☐ A crisis communication protocol: who is notified, who speaks, what the message is
- ☐ Guidance on op-eds, letters to the editor, and public commentary by board members or staff

## Questions to Ask About Your Policy

- Do board members and staff know who the designated media spokesperson is?
- Is there a clear escalation path if a journalist calls a staff member or board member directly?
- Does the policy address what happens when a board member's personal social media activity creates a problem for the organization?
- Is the policy current with the platforms your organization actually uses?
- Has the board discussed the 501(c)(3) implications of political social media content, even from individual board members' personal accounts?
- What is the plan if the organization faces a social media crisis outside of business hours?

**On 501(c)(3) and political activity:**
Tax-exempt nonprofits are prohibited from endorsing or opposing candidates for public office. Social media content — including likes, shares, and reposts — that appears to do this on organizational accounts creates real legal risk. Board members posting political content on personal accounts with organizational affiliation visible is a gray area that your policy should address directly.

---

**A final note on all five policies:**
Policies only protect your organization if they are adopted formally by the board, distributed to everyone they apply to, enforced consistently, and reviewed periodically. A policy binder that sits on a shelf is not governance — it is paperwork. The board's job is to make sure that binder doesn't collect dust.

**Legal disclaimer:**
The information in this guide is intended for educational purposes only and does not constitute legal advice. Nonprofit policy requirements vary by state, organizational size, funding sources, and sector. The questions and frameworks provided here are designed to help boards and executive directors think through their policies — not to substitute for professional legal counsel. Before adopting, amending, or relying on any organizational policy, consult a qualified attorney familiar with nonprofit law in your state.

---

**Need help reviewing your organization's policies or facilitating a board governance conversation?**
Book a free 30-minute discovery call at www.spiegelconsulting.com — or reach Noah directly at noah@spiegelconsulting.com or 615-997-0944.

*© Noah E. Spiegel Consulting 2026 and beyond | All Rights Reserved • This document does not constitute legal or financial advice.*