

Financial & Operational Standards of the National Education Association and Its Affiliates

Modified, September 2026 – NEA/NCSEA

TABLE OF CONTENTS

INTRODUCTION 2

FIDUCIARY RESPONSIBILITIES 3

- Duties of a Fiduciary 3
- Sample Code of Ethical Conduct 3
- Conflict of Interest & Whistleblower Policies 4

FINANCIAL BEST PRACTICES, INTERNAL CONTROLS & OVERSIGHT 5

- Strategic Planning and Budgeting 5
- Financial Reporting and Oversight 5
- Investment Policy Statement 7
- Banking Relationship Standards 8
- Internal Controls and Fraud 9
- Taxable vs. Nontaxable Reimbursements 12
- Expenditures, Purchasing and Disbursements 12
- Audits 13
- AutoPay 15
- Required Tax Filings 15

TECHNOLOGY USE AND INFORMATION SECURITY 16

- Information Security & Privacy Program 16
- Additional Policies and Templates 17
- Document Retention Policy 18
- Considerations for Developing an AI Policy 19

PERIODIC REVIEW FOR STATE AFFILIATES - CHECKLIST 20

ADDITIONAL RESOURCES 21

- Risk Management 21
- Human Resources Policies 21

Membership and Dues 23

The Labor-Management Reporting and Disclosure Act 24

- NEA RA Delegate Elections 24
- Reporting and Filing Obligations 25

Campaign Finance and Lobbying 26

Appendix A – Affiliate Vulnerability Framework 29

DEFENDING EDUCATION

INTRODUCTION

Beginning in 2003, following high-profile financial scandals that led Congress to pass the Sarbanes-Oxley Act to protect shareholders and the public from financial irregularities and fraud, many nonprofit organizations, although not directly subject to Sarbanes-Oxley, voluntarily adopted governance policies designed to promote accountability, transparency, ethical conduct, and compliance with legal requirements. NEA convened a work team of state affiliate leaders and NEA staff that, over several years, developed Financial & Operational Standards, Whistleblower and Conflict of Interest policies for NEA officials and staff, and an Audit Committee Policy.

In 2010, NEA and NCSEA updated the Financial & Operational Standards and published joint guidance, along with model disclosure policies, recommending that all state affiliates adopt them and review them annually. Since that time, the operating environment for nonprofit and labor organizations has evolved significantly. Affiliates face increased expectations regarding governance and financial oversight, cybersecurity and data protection, fraud prevention, records management, whistleblower reporting, regulatory compliance, and enterprise risk management. At the same time, public-sector unions have navigated substantial legal and organizational changes, including the impact of the 2018 Janus v. AFSCME decision and an increasingly complex regulatory and public accountability landscape.

In November 2024, NEA provided NCSEA with an overview of emerging compliance considerations, governance trends, and additional resources available to affiliates. Recognizing the changing landscape, an NCSEA committee convened to review and modernize the guidance in 2025 and 2026.

This joint NEA and NCSEA guidance update the 2010 guide and provide policy templates that may be customized by state and local affiliates. These updated guidelines are intended to help affiliates maintain strong governance practices, safeguard organizational resources and data, strengthen internal controls, promote ethical conduct, and meet evolving legal and operational expectations. We strongly recommend that state affiliates adopt these guidelines, review them annually, and provide periodic training for board members, officers, staff, and local affiliates. Additional resources addressing legal requirements, risk management, cybersecurity, financial stewardship, and operational best practices are also included.

FIDUCIARY RESPONSIBILITIES

DUTIES OF A FIDUCIARY

Affiliate leaders, board members, and staff have legal and ethical responsibilities to the organization. State and local leaders, board members, and some staff are considered fiduciaries under state law and their association's constitution and bylaws. Fiduciaries are given the power to act on behalf of the institution in situations that require great trust, honesty, and loyalty.

The four duties of a fiduciary are care, loyalty, good faith, and fidelity:

Duty of Care: To exercise all the skill, care, and diligence that a prudent person would exercise when acting on behalf of the association; to act in the best interest of the association and in a manner that a prudent person would act under similar circumstances.

Duty of Loyalty: To remain faithful to the association when making decisions and not put one's personal interests above the interests of the association; this includes disclosing any possible conflicts of interest.

Duty of Good Faith: To undertake responsibilities honestly, conscientiously, and fairly; to make decisions in the best interest of all association members and not just for the benefit of one group over another.

Duty of Fidelity: To act in accordance with the association's articles of incorporation, constitution, bylaws, and other governing documents and internal policies, as well as applicable laws and regulations.

SAMPLE CODE OF ETHICAL CONDUCT

In fulfillment of our obligation, we commit to:

1. Exercise appropriate fiduciary responsibilities over Association resources;
2. Not having, directly or indirectly, an interest or relationship, or taking any action or engaging in any transaction, or incurring any obligation, which is in conflict with, or gives the appearance of a conflict with, the proper and faithful performance of our responsibilities;
3. Comply with policies of the Association and applicable laws and regulations;
4. Respect the confidentiality of information acquired in the course of our work;
5. Provide Association constituents with information that is complete, accurate, and appropriate;

6. Carry out activities professionally, with honesty and integrity;
7. Not knowingly be a party to any illegal activity or breach of fiduciary responsibility;
8. Report violations of the Code in accordance with all applicable rules of procedure;
9. Institute policies and procedures that provide for due process for violation of this Code of Ethics;
10. Be accountable for adhering to this Code.

CONFLICT OF INTEREST & WHISTLEBLOWER POLICIES

In furtherance of high ethical standards, officers' and employees' fiduciary obligations, and the importance of transparency and internal controls, NEA adopted Conflict of Interest and Whistleblower policies for both NEA officials and employees. These Conflict of Interest policies provide requirements for NEA officials in their capacity as fiduciaries and for employees to act in the interest of NEA in the course of their employment. The Whistleblower policies establish an expectation and provide a process for NEA officials and employees to report potential misconduct, while protecting them from retaliation for such good-faith reporting. All state affiliates should adopt these policies (see the following model templates):

1) Conflict of Interest Policy Template - Conflict of Interest Polic.docx
2) Whistleblower Policy Template - Whistleblower Policy.docx

DEFENDING EDUCATION

FINANCIAL BEST PRACTICES, INTERNAL CONTROLS & OVERSIGHT

STRATEGIC PLANNING AND BUDGETING

A strategic plan establishes the association's direction, identifies its priorities, and the goals it intends to pursue over a defined period. It should be grounded in the association's mission, vision, and core values: the mission defines why the association exists and whom it serves; the vision describes what the association seeks to achieve or become; and the core values guide how the association carries out its work. The strategic plan translates these foundations into priorities, goals, and actions that guide governance and management decisions.

Financial resources should be aligned with those priorities. The budget is the financial expression of the strategic plan: it identifies the resources necessary to carry out the association's work and demonstrates how member dues and other resources will advance the mission. Strategic planning and budgeting should therefore be interconnected. Before approving a budget, governance should understand not only what the association plans to spend, but why the expenditures are important and how they support strategic priorities.

Governance and management should monitor performance throughout the year by comparing actual results with the approved budget and investigating significant or unexpected variances. Material changes to the financial plan should be communicated to governance and, when appropriate, formally approved.

FINANCIAL REPORTING AND OVERSIGHT

Governance and management should receive timely, accurate, complete, and understandable financial information sufficient to evaluate the association's financial condition and performance. Reporting should allow leaders to understand financial position, operating results, cash and liquidity, performance relative to budget, and significant financial risks. Reports should include appropriate comparisons to prior periods and the approved budget, with explanations of significant or unusual changes.

Governance members are not expected to be accountants, but they are expected to review the information provided, ask questions when something is unclear or unusual, request additional information when necessary, and follow up on unresolved matters. Management has a corresponding responsibility to provide sufficient information and

context for meaningful oversight. Significant financial concerns should be communicated promptly; effective financial reporting should support informed decisions and avoid unnecessary surprises.

Financial Policies

Governance and management should establish and maintain written financial policies appropriate to the association's size, complexity, activities, and risks. Policies define authority and responsibility, promote consistency, protect association resources, and provide continuity when elected leaders or staff change. They should address significant areas of financial activity and risk, including authorization of expenditures, banking, credit cards, reimbursements, reserves, investments, and other material activities.

Governance should approve significant financial policies and review them periodically. Management is responsible for implementing approved policies, establishing supporting procedures, communicating expectations, and informing governance when policies are no longer adequate, or significant exceptions or violations occur. Policies should apply consistently; position, seniority, or elected office should not create an exemption from established financial controls.

Financial Risk Management

Governance and management should periodically identify the significant financial risks facing the association and determine whether appropriate measures are in place to manage them. Risks may arise from declining or concentrated revenue, inadequate reserves, investment losses, litigation, cyber incidents, loss of key personnel, contractual obligations, regulatory noncompliance, inadequate insurance, economic disruption, fraud, or other events that could impair the association's ability to carry out its mission.

Risk management should be integrated into decision-making rather than treated only as a response to a crisis. When a significant risk is identified, leadership should determine whether it should be avoided, reduced through controls or other safeguards, transferred through insurance or contractual arrangements, or knowingly accepted based on the association's circumstances and risk tolerance. Material risks and changes in the risk profile should be communicated to governance in time for informed action.

Reserves

Maintaining adequate financial reserves is an important component of long-term financial health and responsible stewardship. Reserves are financial resources maintained to protect the association’s stability and mission and to provide capacity to respond to

unexpected financial needs or disruptions. As a best practice, the Board should formally designate the assets to be maintained as reserves and establish their purpose and appropriate level through a written reserve policy. Reserves provide the association with financial capacity to withstand unexpected revenue declines, emergencies, litigation, political disruption, cyber events, or other significant pressures without immediately cutting member services, borrowing funds, or making crisis-driven decisions.

Associations should adopt a written reserve policy that establishes the purpose of reserves, the desired level, the funding approach, the circumstances for use, the replenishment expectations, and the responsibility for monitoring and reporting. For state associations, a minimum operating reserve target of approximately 6 months of operating expenses is recommended. For other associations, the appropriate reserve target should reflect the organization's size, financial structure, obligations, and individual risk profile. In determining the appropriate reserve level, leadership should consider revenue predictability, payroll and other fixed obligations, significant financial exposures, access to alternative funding, and the speed at which expenses could be reduced in response to a financial disruption.

Reserves should be intentional rather than simply the result of accumulated cash balances. At the same time, maintaining adequate liquidity is an important component of financial health. An association may have significant net assets but still experience financial difficulty if those assets are concentrated in buildings, long-term investments, or other assets that are not readily available to meet current obligations. Governance and management should ensure that the association maintains sufficient cash and other liquid assets to support operations, meet near-term obligations, and respond to unexpected financial needs.

Leadership should regularly compare reserve balances against the reserve policy target, fund reserves as needed, protect them from inappropriate erosion, and establish a plan to replenish amounts used. Reserve levels, liquidity, and the assumptions underlying the reserve target should be reviewed periodically as the association's financial condition, obligations, and risks of change.

INVESTMENT POLICY STATEMENT

Associations that maintain invested assets should adopt a written Investment Policy Statement (IPS). The IPS establishes a disciplined framework for prudent management and oversight by defining investment objectives, risk tolerance, liquidity needs, time horizon, permitted and prohibited investments, diversification expectations, asset-allocation parameters, performance benchmarks, and decision-making authority.

Before funds are invested, leadership should determine which resources are appropriate for investment. Cash needed for current operations, near-term obligations, or reasonably anticipated expenditures should remain sufficiently liquid and should not be exposed to inappropriate investment risk. Longer-term investment decisions should reflect the purpose of the funds and balance capital preservation, liquidity, risk, and return.

The Board retains ultimate fiduciary responsibility for invested assets even when consultants, advisors, managers, or custodians are retained. The association should understand the services and fees of investment professionals, identify potential conflicts of interest, and monitor compliance with the IPS. Performance should be reviewed regularly against appropriate benchmarks and in the context of the policy's objectives rather than short-term market movements. The IPS should be reviewed at least annually and when significant financial circumstances or organizational priorities change.

BANKING RELATIONSHIP STANDARDS

Associations should establish banking relationships with financially sound, reputable institutions that provide appropriate services, security, accessibility, and support. Accounts should be maintained in the association's name using its EIN, and the association should maintain a current inventory of bank and financial accounts, authorized signers, electronic users, and transaction authorities. Personal accounts should never be used to receive, hold, or disburse association funds.

Banking authority should be clearly defined through policy, resolution, or other governing documents. Access should be based on organizational responsibilities and removed promptly when an officer or employee leaves or changes roles. Banking arrangements should support segregation of duties; whenever practicable, no one person should be able to initiate, approve, and complete a significant transaction without independent review.

Associations should use available fraud-prevention controls appropriate to their risks, such as dual authorization for ACH and wire transfers, transaction limits, Positive Pay or similar services, ACH debit blocks or filters, account alerts, multifactor authentication, and independent review of bank reconciliations. Each user should have unique credentials and only access necessary for their responsibilities. Changes to vendor payment instructions or banking information should be independently verified using trusted contact information.

Leadership should also understand applicable federal deposit-insurance limits and periodically evaluate the concentration of cash, fees, service quality, fraud-prevention capabilities, technology, and the association's future banking needs.

INTERNAL CONTROLS AND FRAUD

Internal controls are the policies, procedures, practices, and oversight mechanisms used to protect assets, promote reliable financial reporting, support compliance, and reduce the risk of error, fraud, or misuse. A strong control environment helps ensure that funds are properly authorized, used for legitimate association purposes, accurately recorded, and independently reviewed. Controls also protect the individuals entrusted with association resources by creating clear expectations and accountability.

No internal control system can eliminate all risks. Controls should provide reasonable assurance that significant errors, irregularities, or inappropriate transactions will be prevented or detected and addressed in a timely manner. When an opportunity for fraud, error, or misuse is identified, the association should establish an appropriate control to mitigate the risk by preventing the activity, detecting it promptly, or reducing its potential impact.

A fundamental principle is segregation of duties. Ideally, authorization, custody or movement of funds, recording, and reconciliation or review are divided among different individuals. No one person should control a financial transaction from beginning to end without independent review. When staffing makes full segregation impractical, compensating controls should provide additional independent oversight. Controls should fit the association's size, complexity, transaction volume, resources, and risk.

Common controls include documented approval requirements, spending limits, timely bank reconciliations, restricted access to financial systems, supporting documentation, dual authorization for significant electronic payments, periodic access reviews, and independent review of financial activity. Controls should be documented, communicated, periodically reviewed, and reevaluated after leadership or staff turnover, system changes, significant growth or decline, or discovery of fraud or control deficiencies.

Tone at the Top

The foundation of an effective internal control system is "tone at the top", the example established by officers, board members, and senior leadership through their words, decisions, and actions. Policies alone cannot create a strong control environment. Leaders must model ethical behavior, transparency, accountability, and compliance with established policies and controls. When leaders follow approval processes, disclose conflicts, ask appropriate questions, respect segregation of duties, and hold themselves to the same standards expected of others, they reinforce a culture of accountability. When leaders circumvent controls, make exceptions for themselves, discourage questions, or

tolerate violations, they weaken the entire system. Trust should never be used as a substitute for internal controls.

Fraud Prevention, Reporting, and Response

Preventing and detecting fraud is a shared responsibility. A strong ethical culture, effective controls, transparent reporting, conflict-of-interest procedures, and a meaningful whistleblower process reduce opportunities for fraud and increase the likelihood that inappropriate activity will be detected. Suspected fraud, theft, misuse, or financial misconduct should be reported promptly through established procedures and evaluated objectively by individuals independent of the matter. Depending on the circumstances, legal counsel, auditors, insurers, law enforcement, or other professionals may need to be involved. Following an incident, leadership should determine how it occurred, whether controls failed or were circumvented, and what corrective action is needed to reduce the likelihood of recurrence.

Credit and Debit Cards

Association credit and debit cards can provide convenience for legitimate business expenses, but they also increase the risk of unauthorized purchases, inadequate documentation, and fraud. Associations should carefully consider whether cards are necessary. Debit cards pose additional risk because transactions generally result in the immediate withdrawal of funds from the association's bank account and may expose association funds to loss more directly. Unless there is a specific business need for a debit card and strong controls governing its use, debit cards are strongly discouraged.

When cards are used, a written policy should define who may possess or use them, allowable and prohibited purchases, spending limits, required approvals, documentation requirements, and procedures for lost, stolen, or compromised cards. Cards, PINs, passwords, and other credentials should never be shared. Cash advances and other cash-equivalent transactions should be prohibited, as should personal expenditures, even when the cardholder intends to reimburse the association.

Associations should also take advantage of fraud-prevention and monitoring tools available through their financial institutions and card providers. Depending on the services available, these may include transaction alerts, spending or transaction limits, merchant-category restrictions, card-locking capabilities, and other controls that allow unusual or unauthorized activity to be identified and addressed quickly.

Every transaction should have an appropriate business purpose and supporting documentation, including an itemized receipt. Card activity should be reconciled and

independently reviewed by someone other than the cardholder or the individual who approved the purchases. Unusual, unsupported, or unauthorized transactions should be investigated promptly, credit card balances should generally be paid in full each billing cycle, and card and system access should be canceled promptly when no longer required.

Gift Cards

Gift cards are frequently used as gifts, awards, incentives, or giveaways, but they raise financial-control, documentation, tax, and accountability concerns because they function as cash equivalents. Once distributed, the association generally has little control over how they are used. Associations should therefore limit their use when practical and establish clear rules for permissible purposes, dollar limits, approvals, and documentation.

When gift cards are purchased, records should track them from purchase through distribution, including the card number and value, purpose, approval, and disposition. Cards provided to identified individuals should be documented by the recipient and the amount; cards used for drawings or member events should be documented in a manner appropriate to the event. Undistributed cards should be secured, inventoried, and reconciled like cash.

Gift cards provided to employees are generally taxable compensation regardless of the dollar amount because cash and cash equivalents do not qualify as de minimis fringe benefits. Gift cards provided to officers, board members, members, or other individuals may also create taxable income and reporting obligations depending on the circumstances. Associations should not assume that a gift card is nontaxable simply because it is described as a gift, award, incentive, or token of appreciation. Appropriate tax treatment and reporting should be determined based on the recipient and purpose of the payment, and associations should consult their tax professional when necessary. Noncash alternatives should be considered when the objective is recognition or appreciation.

Stipends

Associations may provide stipends to officers, board members, members, or others for services or responsibilities undertaken on behalf of the organization. A stipend is generally a fixed or predetermined payment for services and should be distinguished from reimbursement of actual business expenses. Calling a payment "a stipend", honorarium, or consulting fee does not make it nontaxable.

The label given to the recipient also does not determine worker status. Calling an individual a consultant, paying a stipend, or issuing Form 1099 does not automatically make that

person an independent contractor. Before treating a worker as an independent contractor, the association should evaluate the actual relationship, including the degree to which the association directs or controls how, when, or where the work is performed. Misclassification can create employment tax and other liabilities; unclear situations should be reviewed with appropriate tax, payroll, or legal professionals.

Stipends should be formally authorized and documented, including eligibility, purpose, amount or method of determination, frequency, and approval of authority. Care should be exercised when a governing body establishes stipends for its own members or officers. Stipends should remain separate from expense reimbursements and should not be used as a substitute for properly classifying individuals who perform work under the association's direction and control.

TAXABLE VS. NONTAXABLE REIMBURSEMENTS

Under IRS accountable-plan rules, a reimbursement generally must have a legitimate business connection, the individual must adequately account for the expense within a reasonable period, and any excess advance or reimbursement must be returned within a reasonable period. When these requirements are satisfied, qualifying employee reimbursements are not treated as wages for federal income and employment tax purposes.

Associations should require appropriate documentation, including the amount and date of the expense, detailed receipts, and sufficient information to establish the expense's business purpose. Travel and expense policies should identify allowable expenses, approval requirements, documentation standards, applicable mileage or per diem rates, and submission deadlines.

Payments that do not satisfy accountable-plan requirements may be taxable compensation. For example, a fixed expense allowance that does not require substantiation of actual business expenses or return of excess amounts should not automatically be treated as a nontaxable reimbursement. Associations should obtain tax guidance when the treatment of a payment is uncertain.

EXPENDITURES, PURCHASING AND DISBURSEMENTS

Association expenditures should be authorized, reasonable, properly documented, for a legitimate association purpose, and consistent with the approved budget and applicable policies. Policies should establish authority to commit funds, approval limits,

documentation requirements, and circumstances requiring additional approval or competitive bids or quotes.

Invoices and reimbursement requests should be reviewed before payment, and no individual should approve their own expenses. Responsibilities for initiating, approving, recording, and reconciling payments should be separated whenever practical or supported by compensating controls. Changes to a vendor's banking information should be independently verified using trusted contact information, and significant ACH or wire transactions should use dual authorization when available. Transactions should never be divided to circumvent established threshold approval requirements.

Association funds should be traceable from authorization through payment and recording. Every expenditure should have a legitimate business purpose, appropriate approval, sufficient documentation, and independent oversight.

AUDITS

Independent Financial Audit

An independent financial audit is an examination of an association's financial statements by an independent certified public accountant (CPA) or public accounting firm. Its purpose is to provide an objective opinion as to whether the financial statements are presented fairly, in all material respects, under the applicable financial reporting framework. An audit provides independent assurance regarding the reliability of financial information used by governance, management, members, and other stakeholders.

Independent audits are an important component of financial accountability and good governance. During the audit, the auditor considers accounting practices and financial reporting and obtains an understanding of relevant internal controls for purposes of planning and performing the audit. The auditor may communicate control deficiencies, accounting issues, or other matters that warrant attention, giving governance and management an opportunity to address weaknesses.

An audit does not guarantee that fraud, misuse, or every error will be discovered, nor does it transfer responsibility for the financial statements or internal controls to the auditor. Those responsibilities remain with management and governance. An audit should complement, not replace, strong controls, regular financial reporting, and active oversight.

Audit Committee

An audit committee provides independent oversight of the association's financial reporting, external audit, internal controls, tax and regulatory filings, and related financial and compliance risks. It helps the Board fulfill its fiduciary responsibility for the integrity and reliability of financial information while preserving the distinction between management's responsibility for day-to-day operations and governance's oversight role.

The committee should operate under a Board-approved charter or policy defining its authority, composition, responsibilities, and reporting relationship. It should be sufficiently independent of management to exercise objective judgment. The committee should participate in the selection or recommendation of the independent auditor, review the scope and results of the audit, discuss significant findings directly with the auditor, review the audited financial statements and the auditor's communications, and monitor corrective action. It should have an opportunity to meet with the auditor in an executive session without management present.

The committee should also understand significant financial risks and internal controls and review significant tax and regulatory filings, including IRS Form 990 and, when applicable, Department of Labor Form LM-2 and other material returns. Its review should focus on completeness and consistency, significant disclosures, unusual matters, and issues that warrant governance attention. Committee members should receive appropriate orientation and have the authority to seek independent professional advice when necessary.

Independent Financial Expert Qualifications

An audit committee should include at least one individual with sufficient financial knowledge and experience to help the committee evaluate financial reporting, audit results, and the internal control environment. The financial expert's role is not to perform management's or the auditor's work, but to strengthen the committee's ability to ask informed questions, recognize risk, understand audit findings, and evaluate responses.

The individual should have a working understanding of financial statements and generally accepted accounting principles, the purpose and scope of an independent audit, internal and compensating controls, and significant accounting concepts. Expertise may be developed through education, practical experience, or both, and need not depend on a particular credential. Relevant backgrounds may include accounting, auditing, finance, controllership, business management, or other substantial experience in financial reporting and oversight.

The financial expert should be independent of the financial activities being overseen and free from relationships or interests that could reasonably impair, or appear to impair, objective judgment. The presence of a financial expert does not relieve other committee members of responsibility; every member should develop enough financial literacy to participate meaningfully and exercise independent judgment.

AUTOPAY

NEA and all affiliates must adhere to strict legal requirements to secure valid authorizations from our members to collect dues through AutoPay payment methods, including electronic fund transfers from members' bank accounts and recurring credit card charges. NEA's AutoPay platform complies with those requirements. Most affiliates have now executed the *NEA AutoPay Portal: User Agreement*, which outlines the requirements and summarizes potential consequences of not securing legally compliant authorizations.

REQUIRED TAX FILINGS

Compliance with IRS requirements (as well as any state tax law requirements) is crucial for maintaining tax-exempt status. Organizations, including local affiliates, that fail to file an information return (Forms 990, 990-EZ, or 990-N) for three consecutive years are at risk of having their tax-exempt status revoked, which would make their income taxable, and also could lead to audit, further liability, and penalties. State affiliates should ensure that they are scrupulously accurate in preparing their Form 990, and that any applicable taxes are properly paid and reported. They are also encouraged to provide training and reminders to local affiliates, and to periodically monitor locals' tax filing status.

TECHNOLOGY USE AND INFORMATION SECURITY

INFORMATION SECURITY & PRIVACY PROGRAM

All affiliates should have an information security and privacy program to guard against the risk of cybersecurity threats. Not only is this good practice; such measures may be legally required in your state. Since 2018, at least nineteen states have enacted comprehensive consumer privacy laws imposing legal obligations on entities who collect and process the personal information of state residents. At least fifteen of these laws cover 501(c)(5) organizations.[1] In addition, every state has a law requiring businesses to notify individuals if it experiences a data breach exposing certain sensitive personal information to unauthorized persons.

Collectively, these laws may impose substantial compliance requirements on covered affiliates, including requirements to respond to data subject access requests from individuals whose personal information you collect and store; process opt-out or deletion requests; maintain a certain standard of security with respect to your computer systems; provide detailed disclosures about your data processing activities in your online privacy policy; ensure that your contracts with vendors who handle personal information contain specific requirements concerning data security and privacy; and conduct risk assessments for data processing activities that pose increased risks to consumer privacy. In some instances, you may even be required to obtain consent before collecting certain types of personal information.

Most privacy laws are enforced by state attorneys general, and penalties for noncompliance can be substantial where large numbers of records are involved.

The specifics of your information security and privacy program will depend on an individual risk assessment and the applicable laws, but there are several key steps affiliates should take:

[1] As of the date of this guidance, the states that have enacted comprehensive privacy laws covering 501(c)(5) nonprofits are: Virginia, Colorado, Connecticut, Oregon, Texas, Montana, Iowa, Indiana, Delaware, New Jersey, New Hampshire, Nebraska, Maryland, Minnesota, and Rhode Island. Consult your state affiliate legal counsel about the law that may apply in your state.

- Written Information Security Policy (ISP) - Work with competent information technology experts to develop a written information security policy (ISP). This policy serves as the overall framework for protecting your organization's confidential and personal information and should address network security protocols; employee security awareness training; how the affiliate will handle granting data access to third parties; and how the organization will handle confidential business information and personally identifiable information. If you are covered by any comprehensive privacy laws, the law may contain specific requirements for your ISP. A sample ISP is available at Template_Information_Security_Policy.docx.
- Incident Response Plan (IRP) - Develop, test, and implement a written incident response plan (IRP) specifying how the affiliate will respond to security incidents, including cybersecurity incidents. A sample IRP is available at Template_Incident_Response_Plan.docx.
- Data Minimization and Retention Practices - Minimize unnecessary collection and processing of personally identifiable information, unless there is a legitimate business need for that information. Avoid unnecessary collection in the first instance and implement a document retention policy that provides for deletion of information that is no longer needed.
- Third-Party Vendor Security management - Ensure that third-party vendor assessment and contracting practices address information security and personal privacy protections.
- Purchase adequate cybersecurity coverage. You can use this checklist Cyber Insurance Checklist.pdf and coverage rubric Cyber Insurance Coverage Rubric.pdf to assess your coverage needs.
- Ensure your website has an up-to-date privacy notice, as well as cookie consents and opt-out mechanisms if required by applicable privacy laws. This is often the first place state attorneys general look if they want to gauge whether an organization is complying with privacy requirements.

ADDITIONAL POLICIES AND TEMPLATES

Once these basic steps have been completed, additional policies related to technology and information security may be implemented. These may include:

- A Social Media Policy (Template_Social_Media_Policy.docx) - provides guidance on responsible online behavior to protect the affiliate and its reputation.
- Information Technology Acceptable Use Policy (Template_Information_Technology_Acceptable_Use_Policy.docx) - outlines appropriate use of affiliate devices, systems and internet access.

- Artificial Intelligence (AI) Use Guidelines or Policy (Template Guidance for the Responsible Use of Microsoft Copilot.docx) - Establishes requirements for safe and responsible use of AI tools and prohibits sharing sensitive information in unauthorized AI systems.
- Vendor Data Security and Confidentiality Agreement (Template_Data_Security_and_Confidentiality_Agreement_for_vendors.docx) - Helps ensure vendors appropriately protect and maintain the confidentiality of affiliate information.
- Password Policy (Template_Password_Policy_and_Rules.docx) - Establishes requirements for creating, managing, and protecting passwords.

DOCUMENT RETENTION POLICY

Affiliates should develop, adopt, and implement a document retention policy (DRP) that sets guidelines for how long various documents will be retained in an affiliate's files. It also provides that once that period has passed, the document should be destroyed. Having a written policy that is followed helps affiliates manage records and avoid later allegations that documents were destroyed improperly.

Important considerations when creating or updating a DRP include:

• Legal counsel must be involved, as federal, state and local laws will govern how long certain documents must be maintained.

• The DRP should encompass all records in the organization and all media formats, including email communications, texts, and any chat or messaging platforms utilized for work.

• Consistent enforcement is critical -- a DRP that is not consistently enforced does not protect against allegations of bad-faith document destruction.

• Due to the large size of video recordings of virtual meetings and storage costs, best practice is not to record virtual meetings unless absolutely necessary and to routinely delete old recordings.

A template DRP is available here [DRP Template.docx] as a model to review with counsel as your affiliate develops its own DRP.

CONSIDERATIONS FOR DEVELOPING AN AI POLICY

As the use of artificial intelligence (AI) rapidly increases and becomes integrated into a broad range of business applications and tools, affiliates should consider establishing guidelines or policies to support the responsible use of AI. Specific needs will vary depending on how AI is used within an affiliate and are likely to evolve as AI technologies and associated risks continue to change. However, several foundational principles should inform the development of AI policies or guidelines. AI should be utilized in a way that is responsible, secure, accurate, transparent, and accountable. Guidelines are available here: AI Policy Guidelines.docx

DEFENDING EDUCATION

PERIODIC REVIEW FOR STATE AFFILIATES - CHECKLIST

As with any organization, leader transitions are a regular occurrence, and with those transitions, it is recommended that the standard procedures for an affiliate's day-to-day operations be reviewed. It should be noted that even if there isn't a change in leadership, it is a best practice to have a periodic review of the following areas, as indicated:

- Accountability standards
- Employment/HR Guidance
- Building Maintenance:
  - HVAC settings – quarterly
  - Maintenance on major systems (spring and fall)
  - Testing of fire alarms – annually
  - Inspection of elevator functions and regulatory inspections by a third-party vender – annually
  - Inspection of electrical grid – annually
  - Testing of sprinkler system – annually
  - If one is installed, operation of PA system – annually
  - Inspection of building exterior for damage - annually
- Contracting and Purchasing Policies and Procedures Review – A sample of a detailed document can be found here: SAMPLE - NEA Contracting and Purchasing Policies and Procedures - Affiliates .pdf

ADDITIONAL RESOURCES

RISK MANAGEMENT

All state affiliates should have a risk management plan in place – for both cyber and physical security – to provide a safe environment for all staff. Below are samples:

- Incident Response Plan - The importance of having an Incident Response Plan in place is necessary to set forth the organization's protocols for security incident handling, should they occur. It is intended to sharpen an organization's response capability so that it can handle incidents efficiently and effectively, including analyzing incident-related data and determining the appropriate response to each incident. A sample of an Incident Response Plan can be found here: Sample Incident Response Plan.pdf
- Security – It is important that a security plan be put into place, both for specific building security and general security awareness. Sample plans can be found here: SAMPLE General Security Awareness.pdf; Sample Building Emergency Action and Crisis Response Plan.pdf

HUMAN RESOURCES POLICIES

A policy covering anti-discrimination and anti-harassment protects employees and the affiliate. By having a written policy in place, employees are aware of how to report issues, and the policy can be used as part of the affiliate's communications strategy and defense should any incident occur or if litigation is filed involving claims covered by the policy.

An anti-discrimination and anti-harassment policy should:

- State that discrimination and harassment based on protected characteristics is illegal and will not be tolerated.
- Outline protected characteristics. Protected characteristics should be based on federal, state, and local laws.
- Outline prohibited conduct, including what constitutes unlawful harassment and discrimination.
- Be broad based and cover not just employees, but also board members, vendors, visitors, and others.
- Provide how discrimination or harassment should be reported (to any manager or human resources) and that managers are obligated to report any discrimination or harassment to human resources.

- Contain an anti-retaliation provision that protects those who report discrimination or harassment or witnesses who cooperate with an investigation.
- Provide prompt, thorough, and impartial investigation of discrimination and harassment complaints.
- Provide that the confidentiality of employees reporting discrimination or participating in an investigation will be protected to the greatest possible extent.
- The policy should be distributed and available to all employees, and employees should be regularly trained on the policy.

A template policy on anti-harassment and anti-discrimination is available here [Template - Non-Discrimination_Anti-Harassment Policy.docx] as a model to review with counsel as affiliates develop their own policies. An affiliate policy should cover both staff and governance, either in the same policy or in parallel policies.

DEFENDING EDUCATION

MEMBERSHIP AND DUES

Clear, legally compliant membership and dues agreements, along with the consistent application of related policies, are critical components of a strong union. Consult the following NEA resources to assist with developing and updating membership agreements and implementing dues payment platforms:

- *NEA's Model Membership Agreement* (2026): NEA's model unified membership agreement, which is updated annually, brings together best practices from both legal and organizing perspectives to ensure that our membership agreement serves as an effective organizing tool while also providing critical information and disclosures, including those necessary to secure compliant dues authorizations, solicit for political action committee contributions, and obtain permission to text our members.

- *NEA Toolkit on Membership Agreements* (Apr. 2022): NEA's toolkit, revised periodically, provides an in-depth explanation for each portion of the model unified membership agreement, including AutoPay authorization. It also provides guidance on establishing fair and transparent protocols for responding to resignation requests.

- *AutoPay Playbook* (Nov. 2025): NEA's AutoPay Playbook, revised regularly, is designed to help state affiliates plan and execute campaigns to convert members from paying dues through payroll deduction to paying through AutoPay methods, including electronic fund transfers and recurring credit card charges.

THE LABOR-MANAGEMENT REPORTING AND DISCLOSURE ACT

The Labor-Management Reporting and Disclosure Act (LMRDA) governs labor organizations that represent private sector employees. NEA is considered a "mixed labor organization," meaning it has affiliates representing both public- and private-sector employees. All mixed labor organizations are covered by the LMRDA. Labor organizations that solely represent public employees are not covered by the LMRDA. As such, certain state affiliates are covered by the LMRDA because those affiliates are "mixed" and other state affiliates are not covered by the LMRDA because they solely represent public employees. However, all elections for NEA RA delegates are covered by the LMRDA.

NEA RA DELEGATE ELECTIONS

Although affiliates that represent only public sector employees are not generally covered by the LMRDA, their elections of local and state delegates to the NEA Representative Assembly are covered by the LMRDA and must satisfy Title IV's requirements for conducting union officer elections.

Comprehensive guidance for electing NEA RA delegates is updated annually and can be found here: https://www.nea.org/delegaterequirements

For covered state affiliates, key requirements are found under LMRDA Title IV and Title II:

Conducting Union Officer Elections

Title IV of the LMRDA contains election mandates for covered labor organizations. *See* 29 U.S.C. § 481. In general terms, Title IV requires that local unions:

- Conduct officer elections at least every three years;
- Elect officers by secret ballot;
- Provide for general fairness in the election process and nondiscriminatory treatment of candidates running for office;
- Comply with reasonable candidate requests to distribute campaign materials to members;
- Provide union members with adequate advance notice of the opportunity to nominate candidates;
- Provide union member with adequate advance notice of the election; and
- Provide members an opportunity to vote for the candidate of their choosing; and

- Refrain from using any union funds or resources to promote a candidate for office.

As part of the affiliate's election procedures, it is strongly recommended that the affiliate implement a process for filing election complaints that allows them to be reviewed and resolved by the election committee, subject to appeal to the state affiliate.

REPORTING AND FILING OBLIGATIONS

Title II of the LMRDA includes reporting obligations applicable to all covered state affiliates. *See* 29 U.S.C. §§ 431-432. Annually, covered affiliates must file a financial report with the U.S. Department of Labor's Office of Labor-Management Standards (OLMS). The specific financial form (Forms LM-2, LM-3 or LM-4) that an affiliate must complete depends on the value of the organization's annual receipts. These financial reports are due to be filed with OLMS no more than 90 days after the end of the union's fiscal year.

In addition to annual financial reporting, Title II of the LMRDA requires that unions file their governing documents (Constitution and Bylaws) with OLMS. 29 U.S.C. § 431(a). This filing should include the union's current governing documents, so it is recommended that when a union makes significant substantive amendments to the constitution and bylaws, those updated versions are filed with OLMS.

DEFENDING EDUCATION

CAMPAIGN FINANCE AND LOBBYING

Activities that support or oppose any candidates or ballot measures are regulated under campaign finance laws. Elections for federal office are governed by federal law, and elections for state or local offices and ballot measures are governed by state or local laws. Although there are some similarities across federal and state election laws, every state has a unique campaign finance scheme.

Similarly, lobbying for state or local legislation or executive action is regulated under state or local lobbying laws. Lobbying laws vary widely among states, and the triggers for registration and reporting requirements differ by state.

Elections for Federal Office

The Federal Election Campaign Act ("FECA") is the set of campaign finance rules that regulate federal elections. FECA states who can contribute to candidates, parties, and committees and the amount that can be contributed to each. Under FECA, only certain types of entities can make contributions, and contributions must be reported to the Federal Election Commission ("FEC"). Unions may not make any contributions, either monetary or in-kind, to federal candidates, parties, or committees. All federal contributions must be made via a political committee that is permitted to make contributions under FECA and must be reported to the FEC. Federal contributions are funded entirely by voluntary contributions made by members, executive or administrative personnel, and their families.

There are a few exceptions to the prohibition on union contributions: 1) Membership communications, with some exceptions that require certain membership communications still be reported; 2) Free internet communications, but only in the case of federal elections and where there is no paid component (e.g., no "boosting," paying fees for a platform, etc.); 3) Non-partisan Get-Out-The-Vote ("GOTV") and voter registration drives; and 4) Issue advocacy that is focused solely on issues and does not name a candidate.(Note that Legislative advocacy may still be regulated under lobbying laws.)

Elections for State/Local Office

State and local elections are regulated by state campaign finance laws; FECA is not applicable to those elections. Most, but not all, state campaign finance laws prohibit union contributions, including monetary and in-kind, to candidates and parties. For this reason, contributions to state or local candidates and parties should be made via a state political committee that is funded by voluntary political contributions from members. Activity by

the state political committee, including contributor information, is reported to the state or local regulatory agency, typically state elections or ethics boards.

States have varying contribution limits, ranging from very small to unlimited amounts. Additionally, contribution limits for different public offices and parties will usually be different. Coordinating with a candidate or party (*i.e.*, communications made in cooperation, consultation or concert with, or at the request or suggestion of) is considered an in-kind contribution and must be paid for using appropriate PAC funds and will count towards the contribution limit.

Like federal campaign finance law, the vast majority of states do not consider membership communications to be either contributions or expenditures, and they can be coordinated with candidates. Similarly, most states do not regulate nonpartisan communications or issue advocacy.

Independent Expenditures

Independent expenditures are express advocacy communications that are not coordinated with any candidate or party. Express advocacy is defined differently under federal and various state laws but is generally a communication that clearly advocates for or against the election of a candidate for public office. Independent expenditures can be paid for using dues dollars, but paying directly for these communications out of a general treasury can lead to tax liability. Therefore, before engaging in any independent expenditure activities, affiliates should consult with their accountant or tax counsel to determine the tax consequences. Typically, funds should be segregated into a separate fund that is organized under Section 527 of the Internal Revenue Code in order to avoid tax liability. Independent expenditures must be reported to the appropriate regulatory agency, whether that is the FEC or a state or local elections board. Additionally, certain jurisdictions may require that an entity register as an independent expenditure committee in order to engage in independent expenditures. Reporting can also be on an accelerated schedule during a time period close to an election. For example, independent expenditures may be required to be reported within 24 or 48 hours, in addition to regular reports.

Firewall Policies

If a union is running both a coordinated and independent program, or even if they are engaging with partners on independent activities, then they will need to establish a firewall. A firewall is a policy that is set up to prevent the flow of information between staff and officers who are working with candidates and parties (“Coordinated Side”) and staff who are working on independent programs (“Independent Side”). The purpose of a firewall is to ensure that nonpublic information about a candidate or party is not shared with the

Independent Side. A firewall policy should be written, designate those who are on the Independent Side, specify the elections for which the policy is applicable, include the duration of the firewall, and be distributed widely to all staff and relevant board members and officers.

Ballot Measures

Unlike expenditures to candidates or parties, unions may spend unlimited amounts from their general treasuries on ballot measures in any state, subject to any state affiliate agreements to address specific state laws, pursuant to NEA Bylaw 2-7(o). However, while these expenditures are permissible, they are almost always regulated by state or local campaign finance laws. Therefore, if a union intends to participate in ballot measure advocacy, they should review the relevant campaign finance laws to determine whether they will need to register a ballot measure committee and what sort of reporting is due. Unions may also contribute from their general treasury to ballot measure committees, although this may also trigger reporting obligations in a few states.

Lobbying

All states regulate lobbying to some extent, although the degree to which it is regulated varies widely among the states. Nearly all states regulate direct legislative advocacy, meaning direct communication with a legislator about legislation. However, some states also regulate lobbying of the executive office, including administrative officials and quasi-judicial agencies. Additionally, grassroots lobbying (*i.e.*, public communications asking the public to contact a public official about a specific matter) may also be regulated in some states. Where lobbying is regulated, a union and/or an individual being engaged by the union to lobby on its behalf may be required to register as a lobbying organization or a lobbyist and subsequently be required to file lobbying reports. Because some states require registration *prior* to lobbying, affiliates should always review lobbying laws before engaging in lobbying activities.

Ethics/Gift Rules

Many states regulate gifts to public officials under ethics rules. Like lobbying laws, ethics rules vary among the states. Because some states impose extremely strict gift prohibitions (*e.g.*, even minor items such as snacks or light meals may be considered gifts), an affiliate needs to review and understand the ethics rules before providing anything of value to a public official.

APPENDIX A – AFFILIATE VULNERABILITY FRAMEWORK

Appendix A - Affiliate Vulnerability Framework September 2026