Online Financial Safety for PTAs

Online banking and financial tools provide cost and time saving benefits. To enjoy the benefits, and to protect our members' money and security, we must be rigorous in the use of internal controls. Without these controls, the likelihood of fraud is high. Following are some tips and best practices to aid in the development of your PTA's online controls and procedures. Technology is constantly changing, so please review and update your controls regularly.

Important: No online transactions should occur without written procedures and internal controls, which are either clearly stated in your PTA's approved standing rules, or the location of which is referenced in your standing rules. Changes to a PTA's standing rules must be approved by the members of the PTA.

Always refer to the *WSPTA Uniform Bylaws* and the *WSPTA Policy Manual* for the most up to date information. The most current versions of these documents are available on the WSPTA website.

***WSPTA Uniform Bylaws*, Article 5, Section 2 Basic Policies**

E. All financial documents of a local PTA or council including checks and binding agreements shall require the signature of two elected officers. In the event two or more members of the same household hold elected offices in the same local PTA or council, only one member of the household shall co-sign financial documents.

F. Use of a PTA debit card, credit card or ATM card to disburse local PTA or council funds is not permitted. Online banking is allowed in accordance with rules prescribed by WSPTA policy.

WSPTA Policy

Local PTAs and councils may access online banking to review and download monthly bank statements and conduct financial transactions. Local PTAs and councils may accept payments (income) using online sites or in-person devices (e.g. PayPal, Square, etc.) Debit, credit, and ATM cards are not permitted to disburse PTA funds in accordance with the *WSPTA Uniform Bylaws*. Online banking may be used to make electronic payments to cover approved PTA expenses (e.g. nonprofit corporation renewals, etc.).

A local PTA or council board of directors should create and approve written procedures and internal controls for conducting online banking to minimize the risk of misappropriation of funds. The local PTA or council standing rules should also be amended to reflect online banking procedure implementation.

Best practices and effective internal controls will include the following:

- Written commitment by the board of directors to adhere to the controls.
- Written procedures, either clearly stated in the PTA's standing rules, or the location of which is clearly referred to in the PTA's standing rules.
- Requirement of monthly review of all banking/investment accounts by a non-signer/board member.
- Filing system maintained for proper storage of all necessary documentation.
- Organization and consistency.
- Review the PTA's internal control procedures annually.
- Ensure proper training for volunteers.

Following are some areas in which your PTA may want to have specific internal controls.

1. Online Banking

The convenience and mobility of online banking is a benefit most of us enjoy with our personal finances. When working with PTA funds, remember that this money has been entrusted to us by our members. They expect and deserve to have it managed in a secure manner. By doing so, the board is taking its fiduciary responsibility seriously.

Recommended Account Controls

- Consult with the PTA's bank to see what security options are available. PTAs must have signatures of two elected officers on disbursements, so look for a bank that has both a submittal and approval function for online payments.
    - For example, set the two signers' user access according to role and responsibility. Have one signer on the account enter the requested transaction, and the other signer approve the payment. This maintains WSPTA's two signature rule on payments.
- Do not allow the use of shared user names and passwords.
- Assign two bank account signers as administrators.
- Review user access levels annually, and delete user IDs as soon as a signer resigns, or ends his or her term.
- Set up alerts to notify selected persons (suggest president and treasurer, not living in the same household) of payments initiated or deposits made.
- Allow read-only access to the non-signer reviewing the account(s).

Recommended Security Settings

- Install and maintain updated antivirus applications on all computers used to access bank accounts.
- Keep user IDs and passwords safe and secure.
- Never respond to or open Internet links or attachments in unsolicited emails, especially ones that look like they came from your bank.
- Never transfer funds or pay anything from an email request. Phishing scams target PTAs and may appear to come from another officer. Be diligent and talk in person or via phone first with the sender of the request.
- All online payments should require an approved expense request with an invoice or receipt attached, just as for a check payment.

2. Use of ATM, Debit, Credit and Deposit-Only Cards

WSPTA prohibits the use of ATM, debit and credit cards because the risk of fraud is excessive. Deposit-only cards are not necessary, but are allowed. Consult with your bank to find out if this service may be beneficial for your PTA.

3. Accepting Credit Cards

There is increasing demand for PTAs to accept payment via credit cards for dues and other forms of revenue. The accessibility of mobile devices is making this easier, and as long as strong internal controls and accounting practices are in place, this is acceptable. Many services are available and we encourage you to research the cost (fees can add up), benefits, and potential risk to the PTA before using one.

If the PTA chooses to accept credit cards as payment, the PTA is responsible for complying with all rules and procedures required to stay in compliance with Payment Card Industry Data Security

Standards (PCI DSS). If followed, these standards protect the PTA from issues of liability and fraud. PCI Data Security Standards can be found: http://www.pcisecuritystandards.org/securitystandards/pci_dss.shtml

Best Practices

- Do not transmit cardholder's credit data via email, mail, fax, or any other method. Never disclose this information.
- It is a best practice to swipe the credit card rather than hand-keying in the numbers given over the phone or electronically.
- Do not store PIN or other private numbers.
- Do not share user IDs for systems access.
- The PTA's accounting records should reflect both the income from the sale, and the cost of the transaction as an expense. Example: A $15 membership was paid via credit card. The full $15 is recorded as income, and the fee ($.75 for this example – rates may vary) is recorded as an expense.
- Two PTA members should be at the table where credit cards are being processed. Make sure the people taking the credit card information are properly trained. Any person who has access to credit card information is responsible for protecting it.
- Shred all cardholder information once the transaction is complete.
- If a refund is necessary, it must be credited only to the same account from which the payment was made. A process regarding appropriate documentation and refund approval should be included with the PTA's written online banking procedures.

4. Cloud Storage

Cloud storage services allow customers to save data by transferring it over the Internet or another network to an offsite storage system maintained by a third party. This can provide benefits to the PTA, but should be used with caution. Before using a service, research the various providers, and consider:

- Does the cost align with the PTA's budget?
- Can the provider meet the needs of security, availability and size needed by the PTA?
- What is the backup and data recovery assurance? What liability will the PTA incur if the data is lost?
- How user-friendly is the service provider's system? Is it easy to access read, write, save, and delete functions?

Risks

- The provider may be shut down and all data lost if the provider violates state or federal law.
- The PTA must have Internet access to gain access to files.
- Once the data is in the cloud and on the service provider's servers, the PTA no longer physically "owns" the data. If the provider goes out of business for any reason, data may be gone.

Best Practices

- The PTA's written internal control procedures should define who will have access. Once this responsibility is assigned, set up user access rights. This limits who can add, create, or delete files.
- The PTA should maintain a backup schedule to physical devices like hard drives or USB drives. Even if the service provider backs up data regularly, be aware of the risks outlined above.

- Decide on a file storage structure and hierarchy and keep hard copies for anyone who has access. This keeps data organized and easy to find.
- Refer to WSPTA's Record Retention guidelines for which documents must be kept as original hard copies (such as minutes), and proceed accordingly.