NLPSPA Technology Usage Policy

Every Board Director and staff person has access to confidential and private information about the members, work, activities and assets of NLPSPA and as such is in a position of trust to respect the confidential and private nature of all information, including the content of discussions at Board of Director meetings.

Purpose

This policy outlines the acceptable use of technology for board members and staff of the association. It is designed to ensure the responsible and secure use of technology resources, protect against cybersecurity threats, and safeguard the association's information systems and assets.

In recognition of the many beneficial uses of technology in preparation for and participation in meetings of the NLPSPA Board and its various Committees, the Board of Directors will take all necessary measures to protect the confidentiality of the business of the Association during meetings of the Board of Directors and its Committees and to ensure proper and respectful meeting decorum.

Procedures

NLPSPA is committed to a secure, efficient, and environmentally friendly means of storing, organizing and accessing documentation and information related to the business of the Association.

This policy applies to all board members and staff who use the association's technology resources, including but not limited to computers, email accounts, and internet access.

All NLPSPA Board Directors will use laptop devices and other electronic devices for meetings of the Board and regular day-to-day Association business which shall include viewing and reviewing documents relevant to a Board or committee meeting and/or retrieving and/or researching information relevant to a Board discussion or agenda item.

General Use and Ownership

- Any technology resources provided by the association, including, but not limited to, computers, and email accounts, are the property of the association and should be used for association-related purposes only.
- All board members have the option of using an association provided device or a personal device. If a personal device is used for association business it must have the association’s virtual private network (VPN) installed for use when conducting association business and accessing or transmitting association data.
- Personal email addresses must not be used to access or transmit association data, or conduct association business.

- All board members and staff have association provided email addresses that are to be used for conducting association business.
- All board members have the option to have Outlook installed on their personal cell phones if they choose to use them for receiving Association emails. This can provide flexibility and convenience for those who prefer to access their emails on their mobile devices.
- All technology resources should be used in a manner that respects the privacy and rights of others.

User Awareness and Training

- Training updates and refreshers on cybersecurity threats and best practices will be provided by the Association as needed.

Use of Public Wi-Fi Networks

- The Association's Virtual Private Network must be used when connecting to public Wi-Fi networks.
- Automatic connections to public Wi-Fi must be disabled and avoid connecting to unknown Wi-Fi networks when using your Association email account or accessing Association data.

Maintaining Strong Passwords

- Passwords must be strong, unique, and changed immediately upon suspicion or evidence of compromise.
- Two-factor authentication will be implemented wherever possible.
- Use of password managers is encouraged to securely store and manage passwords.

Software and Application Use

- Only use software and applications approved by the association.
- All Association hardware and software must be set to automatically update to ensure the latest security measures are installed.

Encryption and Data Protection

- The association's Microsoft 365 environment is regularly backed up and is equipped with Microsoft Defender for security services.
- Documents and files containing association information or for the purposes of conducting association business are to be stored and managed within the association's Microsoft 365 environment.
- Access to backups is restricted to those who are authorized by the Board for maintenance, testing or restoration activities.

Incident Reporting and Response

- Report any data breaches or security incidents to the association's executive director immediately, who will inform the IT service provider to investigate and action if required.

Meeting Decorum

- Board Directors and staff may maintain access of personal electronic devices during meeting or business hours, provided;
    - They are not used to knowingly transmit, receive, or store any communications that jeopardize the security of the discussions, meeting purpose, or infringe the confidentiality of the business of the Association;
    - Personal devices are placed in silent, mute or vibrate mode during meetings and the member excuses him/herself from the meeting to respond to a call or message;
    - If a Director or staff is expecting an important call or message during a meeting, s/he shall inform the meeting chair of the expected call interruption and exit the meeting at the scheduled time.
    - Board Directors and staff shall be attentive to the business at hand and shall not engage in accessing social media, making personal calls, or sending personal text messaging or emails during meeting or business hours.

Risk Management

- To ensure added protection in the event of a cybersecurity threat the Board of Directors will ensure that the Association has a privacy breach provision included in its annual liability insurance policy.

Monitoring and Compliance

The association reserves the right to monitor the use of its technology resources to ensure compliance with this policy.

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or board membership; Article VII, s.17-19 of the NLPSPA Constitution applies.

Review and Updates

This policy will be reviewed and updated as necessary to ensure it remains effective and relevant.

Approval: Board of Directors, May 30, 2025; this policy replaces the former Electronics Usage Policy