Academy Cloud Storage Security Policy

1. Purpose

The purpose of this policy is to establish guidelines for securely storing, accessing, and managing information in cloud-based platforms used by the American Academy of Orthotists and Prosthetists (the Academy). This ensures the protection of sensitive data related to members, customers, volunteers, and operations.

2. Scope

This policy applies to all individuals with access to the Academy's cloud storage systems, including employees, contractors, and volunteers. It covers data stored, shared, or processed using approved cloud platforms.

3. Acceptable Use

Only cloud services approved by the organization, including Microsoft 365 (employees, and contractors), and Dropbox (volunteers) may be used to store or share organizational information.

Personal cloud accounts must not be used for Academy data under any circumstances. Cloud storage should be used responsibly, with files clearly labeled and organized for collaborative use when appropriate.

Dropbox should be used exclusively for document sharing through the Academy Exchange for the Board of Directors, Councils, Committees, and other groups defined by the Academy.

Only documents used for official business of the Academy should be stored or accessed on the site. Documents of a personal nature or unrelated to Academy business are not allowed.

4. Access Control

Access to cloud folders and documents will be assigned based on roles and responsibilities.
All staff and volunteers accessing cloud systems must use a secure login.
Access will be removed promptly when a staff member or volunteer ends their service or changes roles.

5. Sharing and Permissions

Sharing is limited to specific individuals or groups and regularly reviewed for accuracy.
Files should not be set to "Anyone with the link" unless explicitly approved for access to the cloud folder.

6. Training and Awareness

All employees and volunteers who use cloud platforms will receive basic information on accessing and secure file sharing.

7. Enforcement

Failure to follow this policy may result in revocation of system access, disciplinary action (for employees), or removal from the platform.

8. Review and Revisions

This policy will be reviewed annually by leadership and updated as necessary to address evolving security threats, technological changes, or compliance needs.

9. Document Retention & Archiving

All files and folders will be reviewed regularly to determine continued relevance and compliance with retention requirements.

Unless otherwise noted, files older than five (5) years from the date of creation or last modification will be moved to an Archived Dropbox folder.

Files older than ten (10) years from the date of creation or last modification will be permanently deleted from cloud storage, unless otherwise noted by the staff liaison.

The Archived folder in Microsoft 365 or Dropbox will serve as long-term storage for inactive files that are no longer needed for daily operations but must be retained for reference or compliance purposes.

Files moved to the Archived folder must include a clear naming convention and subfolder structure (Board, council, committee, department or project) and will be accessible only to the staff liaison.

Files that are duplicative, outdated drafts, or otherwise deemed irrelevant may be deleted before the five-year archiving mark, subject to the review by the staff liaison and confirmation by the appropriate body (Board, council, committee, society, etc.).

Staff liaisons are responsible for keeping the folders organized and free of unnecessary content on an ongoing basis.

Appendix A

Dropbox Acceptable Use Policy

All Dropbox users must agree to the Dropbox Acceptable Use Policy

You agree not to misuse the Dropbox services ("Services") or help anyone else to do so. For example, you must not even try to do any of the following in connection with the Services:

- probe, scan, or test the vulnerability of any system or network, unless done in compliance with our Bug Bounty Program;
- breach or otherwise circumvent any security or authentication measures;
- access, tamper with, or use non-public areas or parts of the Services, or shared areas of the Services you haven't been invited to;
- interfere with or disrupt any user, host, or network, for example by sending a virus, overloading, flooding, spamming, or mail-bombing any part of the Services;
- access, search, or create accounts for the Services by any means other than our publicly supported interfaces (for example, "scraping" or creating accounts in bulk);
- send unsolicited communications, promotions or advertisements, or spam;
- send altered, deceptive or false source-identifying information, including "spoofing" or "phishing";
- promote or advertise products or services other than your own without appropriate authorization;
- abuse referrals or promotions to get more storage space than deserved or to sell storage space received from referrals or promotions;
- circumvent storage space limits;
- sell the Services unless specifically authorized to do so, or purchase the Services from an unauthorized seller;
- use the Services to back up, or as infrastructure for, your own cloud services;
- use the storage space provided by the Services as the basis for cryptographic proof-of-space or proof-of-storage, or any similar proof system;
- engage in any type of payment fraud, including unauthorized use of credit cards or other payment methods, illegitimate chargebacks, or any other method of obtaining the Services without required payment;
- publish, share, or store materials that constitute child sexually exploitative material (including material which may not be illegal child sexual abuse material but which

nonetheless sexually exploits or promotes the sexual exploitation of minors), unlawful pornography, or are otherwise indecent;

- publish, share, or store content that contains or promotes extreme acts of violence or terrorist activity, including terror or violent extremist propaganda;
- advocate bigotry, hatred, or the incitement of violence against any person or group of people based on their race, religion, ethnicity, national origin, sex, gender identity, sexual orientation, disability, impairment, or any other characteristic(s) associated with systemic discrimination or marginalization;
- harass or abuse Dropbox personnel or representatives or agents performing services on behalf of Dropbox;
- violate the privacy or infringe the rights of others, including publishing, sharing, or storing other people's confidential information, identifying information, or intimate imagery without authorization for the purposes of harassing, exposing, harming, or exploiting them;
- otherwise violate the law in any way, including storing, publishing, or sharing content which depicts, promotes, or instructs on illegal activity, is fraudulent, defamatory, misleading, or exploitative, or that infringes the intellectual property rights of others.

Dropbox endeavors to enforce our policies fairly and consistently. We reserve the right to take swift and appropriate action in response to violations of this policy, which could include removing or disabling access to content, suspending a user's access to the Services, or terminating an account.