Sylvan Lake Minor Ball Association

Information Security & Cyber Safety Guide

1. Protect Account Access

• Use strong passwords (12+ characters, mix of letters, numbers, and symbols).
• Never reuse passwords from other sites.
• Turn on Multi-Factor Authentication (MFA) for Microsoft accounts.
• Don’t share login credentials — every board member should have their own account.

2. Handle Sensitive Information Carefully

• Only store personal or financial data in SharePoint/OneDrive.
• Restrict access to documents — only those who need them should have it.
• Avoid downloading or forwarding sensitive files.
• Remove access for board members who leave.

3. Email & Phishing Awareness

• Be suspicious of emails asking for money, gift cards, or urgent action.
• Don’t click links or open attachments from unknown senders.
• Double-check sender email addresses.
• Report suspicious emails to the board.

4. Device Security

• Keep devices updated — turn on automatic updates.
• Use antivirus or built-in protection (like Windows Defender).
• Lock screens when away from your device.
• Avoid public Wi-Fi for board work.

5. File & Folder Permissions

• Share files using “specific people” instead of “anyone with the link.”
• Review permissions each season.
• Keep a list of who has admin access.
• Perform an access audit annually.

6. Incident Response

• If something goes wrong (hack, lost file, etc.), notify the board immediately.
• Change your password right away.
• Revoke document access if needed.
• Report to Microsoft support if serious.
• Review and learn from the event.

7. Good Data Hygiene

• Delete outdated documents (e.g., old rosters or forms older than 2 years).
• Use clear, consistent file names.
• Avoid storing unnecessary personal data.
• Clean up your OneDrive each season.

8. Training & Awareness

• Review this guide once per year.
• Discuss security issues or incidents at a board meeting each season.
• Encourage questions — it’s better to double-check than make a mistake.