Sawyer STREAM Academy
7901 4th Street N, Suite 25745, St. Petersburg, FL USA 33702
contact@sawyer-academy.org | www.sawyer-academy.org

CYBERSECURITY POLICY

Protection of Systems, Accounts, Communications, and Educational Data

School	Sawyer STREAM Academy
Legal Organization	Sawyer Scholastics, LLC
Policy Owner	Executive Director
Approved By	Dr. Robert Sawyer
Effective Date	1 August 2026
Review Cycle	At least annually and after any significant cybersecurity incident or material technology change

This policy establishes the cybersecurity responsibilities and safeguards used to protect Sawyer STREAM Academy's distance-learning environment, student and staff accounts, educational systems, communications, and institutional information.

1. Purpose

Sawyer STREAM Academy depends on secure, reliable technology to deliver instruction, maintain student records, communicate with families, support employees, and conduct school operations. This policy establishes a coordinated approach to preventing, identifying, reporting, containing, and recovering from cybersecurity threats that could interfere with those responsibilities.

The Academy seeks to protect the confidentiality of information, the integrity and accuracy of systems and records, and the availability of educational services. Cybersecurity decisions are guided by reasonable risk management, the best interests of students, the Academy's Culture of Care, and the operational needs of a distance-learning school.

2. Scope

This policy applies to administrators, employees, teachers, contractors, consultants, volunteers, partner-school personnel, students, parents or guardians, and service providers who use or access Sawyer STREAM Academy systems, accounts, devices, networks, records, communications, or approved educational applications.

It applies to school-managed and personally owned devices used for school purposes, including computers, tablets, mobile devices, storage media, email accounts, learning platforms, student information systems, video-conferencing tools, cloud services, and other approved technologies.

3. Cybersecurity Governance and Responsibility

The Executive Director provides institutional oversight for cybersecurity. The Executive Director may assign technical, administrative, or incident-response responsibilities to qualified personnel or approved service providers. Academic leaders and supervisors are responsible for ensuring that personnel under their direction follow this policy and complete required training.

Every user shares responsibility for protecting the Academy's digital environment. Users must follow security instructions, safeguard credentials, use only approved systems for school information, and promptly report suspected security concerns.

4. Risk-Based Security Approach

Sawyer STREAM Academy applies safeguards according to the sensitivity of information, the importance of the system, the likelihood and potential impact of a threat, available technical controls, and the needs of students and staff. Higher-risk systems, including systems containing student records or administrative credentials, receive stronger access restrictions and closer oversight.

Cybersecurity risk is reviewed as part of technology planning, vendor selection, system implementation, policy review, and incident follow-up. The Academy may strengthen controls when risks, technology, legal requirements, or operating conditions change.

5. Account Creation and Access Control

Access to school systems is granted only for legitimate educational or operational purposes. Each authorized user should have an individual account when the system supports individual accounts. Shared accounts are avoided unless operationally necessary and specifically authorized.

Permissions are based on role and legitimate need. Access is adjusted when responsibilities change and removed promptly when enrollment, employment, service, or authorization ends. Administrative privileges are limited to persons whose responsibilities require them.

6. Passwords and Authentication

Users must create strong passwords or passphrases and must not disclose them to unauthorized persons. Passwords should not be reused across unrelated services. Default passwords must be changed before an account or device is placed into regular use.

Multi-factor authentication is required for administrative and staff accounts when supported by the applicable system and reasonably available. It may also be required for other users or systems based on risk. Suspected compromised credentials must be changed immediately and reported.

7. Device Security

Devices used to access school systems must be maintained in a reasonably secure condition. Operating systems, browsers, applications, and security software should be kept current. Screen locks, passwords, or equivalent protections should be enabled when available. Devices should not be left accessible to unauthorized persons.

Users must not disable security features, install malicious or unauthorized software, or connect compromised devices to school systems. Lost or stolen devices that may contain school information or active school credentials must be reported promptly.

8. Secure Use of Email and Communications

Official school business should be conducted through approved communication channels. Users must exercise caution with unexpected messages, links, attachments, requests for payment, requests for credentials, and communications that create unusual urgency or pressure.

Confidential student, family, employee, or business information must not be transmitted through personal accounts or unapproved messaging services. Sensitive information should be limited to the minimum necessary and shared only with authorized recipients.

9. Phishing, Social Engineering, and Fraud Prevention

Users are expected to recognize and report phishing, impersonation, fraudulent payment requests, account takeover attempts, suspicious login notices, and other social-engineering activity. Requests involving money, credentials, confidential information, or changes to payment instructions must be independently verified through an established communication channel.

No user should approve a financial transaction, release confidential information, or change account access solely on the basis of an unexpected electronic request.

10. Data Protection and Encryption

Student and institutional information must be handled in accordance with the Student Data Privacy Policy and related records procedures. Information is stored only in approved locations and is shared only for authorized purposes.

Where supported and appropriate, the Academy uses encrypted transmission, secure websites, protected cloud storage, and device or file encryption. Portable storage media containing confidential information should be avoided; when necessary, its use must be authorized and appropriately protected.

11. Approved Software, Applications, and Cloud Services

Only approved applications and services may be used to store, process, or transmit confidential school information. Before adoption, the Academy considers educational purpose, data practices, access controls, security features, reliability, technical support, and compatibility with school operations.

Personnel may not independently create accounts for students or upload student information to unapproved platforms. Trial use involving real student data requires prior authorization.

12. Vendor and Service-Provider Security

Technology providers that access or process school information are selected with attention to their security practices, privacy terms, service reliability, support, and ability to meet Academy requirements. Where feasible, agreements or terms should address authorized use, confidentiality, incident notification, data return or deletion, and restrictions on commercial exploitation.

Provider access is limited to what is necessary. The Academy may review provider performance, security notices, significant service changes, and known incidents when deciding whether continued use is appropriate.

13. Backups and Recovery

Important school records and systems are backed up or otherwise preserved according to operational need and system capability. Backup arrangements are intended to support recovery from accidental deletion, device failure, malicious activity, service interruption, or other disruption.

Backup access is restricted. Recovery procedures are reviewed periodically and may be tested when practical. Critical academic and administrative records should not depend on a single unprotected device or account.

14. System Updates, Configuration, and Maintenance

Software updates, security patches, and system configuration changes are applied within a reasonable period according to risk, vendor guidance, system importance, and operational

impact. Unsupported or obsolete systems are replaced, isolated, or subject to additional controls when continued use is temporarily necessary.

Administrative settings, account permissions, integrations, and security options are reviewed periodically and whenever a significant system change occurs.

15. Monitoring and Logging

The Academy may maintain system, access, communication, and security logs for legitimate educational, operational, safety, and cybersecurity purposes. Monitoring is limited to authorized purposes and is conducted with respect for privacy and applicable policy.

Logs may be reviewed to investigate suspected account misuse, unauthorized access, data loss, cyberbullying, malware, service disruption, or other policy violations. Users should not expect privacy when using school-managed systems beyond the protections established by school policy and applicable law.

16. Cyberbullying, Harassment, and Harmful Digital Conduct

Cybersecurity includes protecting students and staff from harmful use of digital systems. Threats, impersonation, harassment, cyberbullying, unauthorized recording, publication of private information, malicious account access, and deliberate disruption of online learning are prohibited.

Reports involving student safety or harmful conduct are addressed under the Digital Safeguarding Policy, Student Conduct and Respectful Communication Policy, Student Crisis Response Policy, and other applicable procedures.

17. Security Incident Reporting

Any suspected cybersecurity incident must be reported promptly through an official school communication channel. Reportable concerns include suspicious messages, compromised credentials, unauthorized access, lost devices, malware, unexpected system behavior, data disclosure, account impersonation, denial of service, and unexplained changes to records or settings.

Users should preserve relevant messages, screenshots, dates, times, usernames, and other information when it is safe to do so. Users must not conduct their own intrusive investigation, contact a suspected attacker, or delete relevant evidence unless directed by authorized personnel.

18. Incident Response

When a cybersecurity concern is reported, the Academy will assess the situation, determine the potential effect on students and operations, contain the risk, protect or preserve relevant evidence, coordinate with service providers when needed, and restore affected services in a controlled manner.

Response actions may include account suspension, credential resets, access restrictions, device isolation, vendor notification, recovery from backups, correction of records, family or stakeholder communication, law-enforcement or regulatory consultation when appropriate,

and additional training. Notifications are made when required or when leadership determines that communication is necessary to protect affected persons.

19. Business Continuity and Educational Continuity

Cybersecurity incidents may affect access to instruction, communication, records, or school services. The Academy maintains reasonable continuity procedures for priority functions, which may include alternate communication channels, temporary instructional arrangements, offline records, recovery priorities, and coordination with technology providers.

Leadership determines when systems may safely return to normal use and communicates temporary procedures to affected users.

20. Cybersecurity Awareness and Training

Personnel with access to school systems receive orientation and periodic training appropriate to their responsibilities. Training may address password security, multi-factor authentication, phishing, secure communication, student-data protection, device security, incident reporting, cyberbullying, and safe use of online instructional tools.

Students and families receive age-appropriate guidance on account safety, suspicious messages, privacy, responsible technology use, cyberbullying, and reporting concerns. Additional training may be required following an incident or when significant risks are identified.

21. Remote Work and Distance-Learning Security

Because Sawyer STREAM Academy operates through distance learning, users often access systems from homes, partner schools, and other locations. Users must take reasonable steps to prevent unauthorized viewing, discussion, recording, or access to confidential information in these settings.

Public or unsecured networks should be avoided for sensitive activity when a safer option is available. Users should log out of shared devices, protect screens and conversations from unauthorized persons, and securely store any printed records.

22. Prohibited Activities

Users may not attempt to bypass security controls, obtain another person's credentials, access information without authorization, introduce malicious software, interfere with services, scan or test systems without approval, conceal identity for harmful purposes, or use Academy systems for unlawful activity.

Users may not copy, disclose, alter, destroy, or remove school information without authorization. Security research, vulnerability testing, and administrative tools may be used only by authorized personnel or approved service providers.

23. Enforcement and Corrective Action

Violations of this policy may result in removal of access, required training, corrective action, disciplinary consequences, termination of employment or services, suspension or termination of enrollment, and referral to appropriate authorities when warranted.

Responses are determined according to the seriousness of the conduct, the risk or harm created, the user's role and age, intent, prior history, and applicable school policies. Corrective action may also include restoring records, strengthening controls, or revising procedures.

24. Review and Continuous Improvement

This policy is reviewed at least annually and after significant cybersecurity incidents, material system changes, or identified weaknesses. The review may consider incident trends, training completion, account and access reviews, vendor performance, system changes, stakeholder feedback, and recommendations from qualified advisers or external reviewers.

Revisions are approved through the Academy's governance process and communicated to personnel, students, families, and service providers as appropriate.

25. Cybersecurity Responsibility Matrix

Role	Primary Responsibility	Examples of Implementation Evidence
Executive Director	Policy approval, risk oversight, incident escalation, continuity decisions	Approval records, annual reviews, incident decisions, corrective actions
Academic Directors	Secure academic practices, staff guidance, appropriate use of instructional systems	Training records, course-system reviews, access approvals
Technology Support / Providers	Account controls, updates, backups, technical response, service restoration	Access logs, support records, patch records, backup and recovery documentation
Teachers and Staff	Credential protection, secure communication, appropriate data handling, prompt reporting	Acknowledgments, training records, incident reports
Students and Families	Safe account use, responsible technology behavior, reporting concerns	Orientation completion, signed acknowledgments, reports and communications

26. Implementation Evidence Maintained by the Academy

To demonstrate implementation of this policy, Sawyer STREAM Academy maintains evidence appropriate to its operations, which may include:

- Current approved policy and revision history;
- Cybersecurity orientation and training records;
- User access, account review, and account termination records;
- Multi-factor authentication and administrative-access records where applicable;

- Approved software and service-provider inventory;
- System update, maintenance, backup, and recovery documentation;
- Cybersecurity incident reports, response records, notifications, and corrective actions;
- Continuity procedures and service-restoration records;
- Student and family digital-safety orientation or acknowledgment records; and
- Annual cybersecurity review and improvement documentation.

27. Policy Acknowledgment

The undersigned acknowledge that they have received or been provided access to the Sawyer STREAM Academy Cybersecurity Policy and understand the responsibilities applicable to their role.

Name	
Role / Relationship to Student	
Signature	
Date	
Student Name, if applicable	