



Digital Safeguarding Policy

Protection, responsible participation, and safe learning in the online environment

Sawyer STREAM Academy is committed to providing a secure, respectful, and developmentally appropriate digital learning environment in which students can learn, communicate, create, and participate with confidence.

Policy owner	Executive Director
Applies to	Students, families, employees, contractors, volunteers, and partner-school personnel
Approval date	1 August 2026
Effective date	1 August 2026
Review cycle	At least annually and whenever significant legal, operational, or technology changes occur
Version	1.0



1. Purpose

This policy establishes the safeguards Sawyer STREAM Academy uses to protect students while they participate in online instruction, digital communication, assessment, school activities, and other technology-supported services. It defines expected conduct, prevention measures, reporting procedures, response responsibilities, and the shared roles of the Academy, students, families, employees, contractors, volunteers, and partner schools.

Digital safeguarding is broader than cybersecurity. It includes protection from harassment, exploitation, grooming, bullying, inappropriate content, unsafe communication, privacy violations, identity misuse, and other conduct that may place a student at risk in a virtual environment.

2. Scope

This policy applies whenever a person uses an Academy account, platform, learning management system, student information system, video-conferencing tool, messaging service, email account, shared document, digital resource, or other technology connected to Sawyer STREAM Academy. It also applies to off-platform conduct when that conduct substantially affects student safety, access to learning, or the orderly operation of the Academy.

3. Guiding Principles

- Student welfare takes priority over convenience, reputation, or informal resolution.
- Online interactions must reflect the Academy mission, Family Values, and Culture of Care.
- Adults must maintain clear professional boundaries and use approved communication channels.
- Students should be taught how to recognize risk, ask for help, and participate responsibly.
- Reports must be taken seriously, documented promptly, and addressed without retaliation.
- Only information necessary to protect the student and resolve the concern should be shared.

4. Definitions

Digital safeguarding: The policies, practices, supervision, education, and response measures used to protect students in online and technology-supported environments.

Cyberbullying: Repeated or serious digital conduct intended to threaten, humiliate, exclude, harass, or harm another person.

Grooming: A pattern of conduct through which a person builds access, trust, secrecy, or emotional dependence for an exploitative or abusive purpose.

Inappropriate content: Material that is sexually explicit, violent, hateful, discriminatory, exploitative, illegal, age-inappropriate, or inconsistent with legitimate educational purposes.

Personal data: Information that identifies or can reasonably be linked to a student or family.



Safeguarding concern: Any observation, disclosure, message, image, behavior, or pattern suggesting that a student may be unsafe, exploited, threatened, abused, or at risk.

Approved platform: A system authorized by Sawyer STREAM Academy for instruction, communication, assessment, records, or school activities.

5. Roles and Responsibilities

5.1 Executive Director

The Executive Director maintains institutional responsibility for digital safeguarding, approves related policies and response procedures, designates responsible personnel, ensures staff training, and determines when outside authorities, service providers, or legal counsel must be contacted.

5.2 Designated Safeguarding Personnel

Designated personnel receive and document reports, assess immediate risk, preserve relevant evidence, coordinate protective measures, communicate with families when appropriate, and maintain confidential safeguarding records. When a concern involves designated personnel, the report must be directed to the Executive Director or another independent responsible person.

5.3 Employees, Contractors, and Volunteers

All adults working with students must use approved systems, maintain professional boundaries, supervise online interactions appropriately, protect confidential information, and report safeguarding concerns promptly. They must not investigate a serious allegation independently, promise secrecy, or attempt to resolve a risk informally when formal reporting is required.

5.4 Students

Students are expected to communicate respectfully, protect passwords and personal information, use school systems for legitimate educational purposes, avoid sharing harmful or inappropriate content, and report concerns involving themselves or others.

5.5 Parents and Guardians

Families are expected to support safe device use, help students maintain appropriate learning spaces and routines, review Academy expectations, communicate concerns promptly, and cooperate with reasonable safeguarding measures.

6. Safe Communication and Professional Boundaries

Employees and other authorized adults must communicate with students through Academy-approved accounts and platforms whenever reasonably possible. Communication must be connected to a legitimate educational or student-support purpose, use professional language, and occur at reasonable times except in an emergency or time-sensitive safeguarding situation.

- Private or disappearing-message applications may not be used for routine school communication unless expressly approved.



- Adults may not request secrecy from students or engage in romantic, sexual, coercive, exploitative, or otherwise inappropriate communication.
- One-to-one video sessions should use approved platforms and follow Academy procedures regarding scheduling, visibility, documentation, and family awareness.
- Personal social-media connections between employees and currently enrolled students are prohibited unless specifically authorized for an official school purpose.
- Recording, photographing, or distributing a student image, voice, work product, or personal information requires a legitimate school purpose and appropriate authorization.

7. Online Instruction and Video-Conferencing Safeguards

Teachers and facilitators must use meeting controls appropriate to the age of students and the purpose of the session. Links and access codes should not be posted publicly. Participants must use identifiable names, and unauthorized persons may be removed. Screen sharing, chat, breakout rooms, recording, and file transfer should be enabled only when educationally appropriate and reasonably supervised.

Students should participate from an appropriate location and should not display private household information, confidential documents, or other people without permission. Families should notify the Academy when a student requires an accommodation or alternative participation arrangement.

8. Student Digital Conduct

Students must not use Academy systems to threaten, harass, impersonate, deceive, exclude, exploit, or embarrass another person. They may not attempt to bypass security controls, gain unauthorized access, distribute malicious code, share passwords, submit another person's work, or interfere with instruction or school operations.

Students must not create, request, possess, or distribute sexual images of minors, threats of violence, hateful content, or material that promotes self-harm. Any student who receives such material should avoid forwarding it, preserve the message when safe to do so, and report it immediately to a trusted adult or school representative.

9. Privacy and Data Protection

Sawyer STREAM Academy limits collection and use of student information to legitimate educational, administrative, legal, and safety purposes. Access is restricted according to role and need. Users must protect passwords, devices, records, and confidential communications from unauthorized access or disclosure.

Suspected loss, theft, unauthorized access, accidental disclosure, or misuse of student information must be reported promptly. Data-related incidents are handled in coordination with the Academy's Student Data Privacy Policy, Cybersecurity Policy, and applicable records procedures.



10. Prevention and Education

The Academy provides age-appropriate guidance on safe passwords, phishing, privacy, digital footprints, respectful communication, cyberbullying, misinformation, inappropriate content, help-seeking, and reporting. Employees receive training on professional boundaries, warning signs, response procedures, confidentiality, and documentation. Families receive information that helps them reinforce safe online practices at home.

11. Recognizing Safeguarding Concerns

A safeguarding concern may arise from a direct disclosure, a change in behavior, unusual withdrawal, threatening or sexual messages, pressure to keep secrets, requests for personal images, impersonation, repeated harassment, unexplained account activity, references to self-harm, or other signs that a student may be unsafe. No single sign proves that harm has occurred, but concerns should not be dismissed merely because information is incomplete.

12. Reporting Procedures

A student, family member, employee, contractor, volunteer, or partner-school representative may report a concern verbally or in writing through an approved school communication channel. Reports should include the names of involved persons, date and time, platform used, description of what occurred, and any available screenshots, messages, links, or other evidence.

A person who believes there is an immediate danger should contact the appropriate local emergency authority first and then notify the Academy. Because Sawyer STREAM Academy serves students in multiple locations, emergency response may require coordination with the student's parent or guardian, partner school, or local authority in the student's jurisdiction.

13. Response to Reports

Response stage	Required action
Immediate safety assessment	Determine whether the student faces urgent danger and take reasonable protective action.
Documentation	Create a confidential record of the report, evidence received, actions taken, and persons notified.
Preservation of evidence	Secure relevant messages, files, account information, meeting records, and other materials without unnecessary distribution.
Interim safeguards	Restrict contact, remove access, adjust course arrangements, provide supervision, or take other temporary measures when necessary.



Response stage	Required action
Notification and referral	Inform parents or guardians when appropriate and contact service providers, law enforcement, child-protection authorities, or other agencies when required or reasonably necessary.
Review and determination	Assess the available information fairly, protect confidentiality, and determine corrective, disciplinary, supportive, or preventive action.
Follow-up	Check student safety, document outcomes, restore access when appropriate, and evaluate whether policies or controls should be improved.

14. Support for Affected Students

The Academy responds to safeguarding concerns with attention to both safety and continued access to education. Support may include a designated adult contact, adjusted communication arrangements, academic flexibility, counseling referral information, family conferences, technology support, or coordination with a partner school or local service provider. Support is determined according to the circumstances and the Academy's available services.

15. Corrective and Disciplinary Action

Violations may result in loss of technology privileges, required training, restricted communication, removal from an activity or course environment, behavioral intervention, suspension, termination of enrollment, employment action, contract action, or referral to appropriate authorities. The response should consider student age, intent, severity, repetition, impact, safety, and applicable policy or law.

16. Confidentiality and Non-Retaliation

Safeguarding information is shared only with persons who have a legitimate need to know. Absolute confidentiality cannot be promised when disclosure is necessary to protect a student, conduct a fair review, comply with law, or obtain professional assistance. Retaliation against a person who makes a good-faith report, participates in a review, or seeks help is prohibited.

17. Recordkeeping

Safeguarding reports, evidence, decisions, notifications, and follow-up actions are maintained separately from ordinary instructional communications when appropriate and are protected against unauthorized access. Records are retained according to Academy policy, legal requirements, and the need to document student protection actions.



18. Third-Party Platforms and Service Providers

Before adopting a digital platform that will be used by students, the Academy considers educational purpose, privacy and security practices, age appropriateness, account controls, moderation tools, accessibility, and available support. No platform can eliminate all risk; therefore, approval does not replace supervision, responsible use, or prompt reporting of concerns.

19. Training, Review, and Continuous Improvement

This policy is reviewed at least annually and after any significant safeguarding incident, technology change, or relevant legal development. The review may consider incident patterns, user feedback, training completion, platform performance, stakeholder concerns, and recommendations from qualified professionals. Revisions are approved through the Academy's established governance process and communicated to affected stakeholders.

20. Related Documents

- Student Data Privacy Policy
- Cybersecurity Policy
- Technology Acceptable Use Policy
- Student Crisis Response Policy
- Student Conduct and Respectful Communication Policy
- Admissions Policy
- Student Orientation Guide
- Parent and Family Orientation Materials
- Academic Integrity Policy



Sawyer STREAM Academy

Sawyer Scholastics, LLC | 7901 4th Street N, Suite 25745 | St. Petersburg, FL USA 33702

Digital Safeguarding Acknowledgment

I acknowledge that I have received or been given access to the Sawyer STREAM Academy Digital Safeguarding Policy. I understand that students, families, and school personnel share responsibility for maintaining a safe and respectful online learning environment. I understand how to report a concern and agree to cooperate with reasonable safeguarding procedures.

Student name:

Parent/guardian name:

Student signature:

Date:

Parent/guardian signature:

Date:

Academy representative:

Date:

Policy Approval

Approved by Dr. Robert Sawyer

Signature

Date 1 August 2026