

Children's Internet Protection Act (CIPA)

Internet Safety Policy

Policy Name: CIPA Internet Safety Policy

Applies To: Students, staff, volunteers, and other authorized users of school technology and network resources

Responsible Administrator: Head of School / School Administrator

Review Cycle: Annual

Effective Date: 9/4/26

Approved By: Board of Directors

Approval Date: 9/4/26

1. Purpose

Heartwood Montessori is committed to providing students with safe, developmentally appropriate access to technology and online resources that support learning, exploration, creativity, communication, and responsible participation in the digital world.

This policy establishes safeguards for the use of the School's internet access, networks, devices, and digital resources and is intended to support compliance with the **Children's Internet Protection Act (CIPA)** and applicable E-Rate requirements.

Our approach to internet safety reflects both our legal responsibilities and our educational commitment to helping children develop independence, responsibility, sound judgment, and respect for themselves and others.

2. Technology Protection Measures

Heartwood Montessori will maintain technology protection measures, including internet filtering or blocking technology, on school computers and networks with internet access as required by CIPA.

The technology protection measures are designed to block or filter access to visual depictions that are:

- Obscene;
- Child pornography; or
- Harmful to minors, when accessed by minors.

The School may also restrict access to websites, applications, online services, or categories of content that it determines are inappropriate for students, inconsistent with the educational mission of the School, disruptive to the learning environment, or reasonably likely to present a safety or security risk.

Filtering technology is an important safeguard but is not a substitute for student education, responsible adult supervision, or appropriate student behavior.

For adult users, an authorized administrator or other authorized individual may disable a technology protection measure when permitted by law for bona fide research or another lawful purpose.

3. Student Internet Access

Student access to the internet and school technology is provided for educational purposes.

Students are expected to:

- Use technology in ways consistent with classroom expectations and school values;
- Follow the directions of guides, teachers, and other authorized staff;
- Access websites, applications, and digital resources appropriate to their learning;
- Treat others respectfully when communicating electronically;
- Protect passwords and account information;
- Respect the privacy and personal information of others;
- Report inappropriate, unsafe, threatening, or concerning online content or interactions to a trusted adult; and
- Use school technology in a manner that does not interfere with the learning or safety of others.

Access to school technology is a privilege and may be limited or suspended when technology is misused.

4. Access to Inappropriate Online Material

Heartwood Montessori will take reasonable measures to prevent minors from accessing inappropriate matter on the internet and World Wide Web.

The School will use a combination of:

- Technology protection and filtering measures;
- Developmentally appropriate supervision;
- Classroom expectations and procedures;
- Digital citizenship and internet safety education; and
- Staff intervention when inappropriate material is encountered.

If a student inadvertently encounters inappropriate content, the student should leave or close the content when possible and promptly notify a staff member.

5. Safety in Electronic Communications

Students will receive developmentally appropriate guidance regarding safe participation in electronic communications, including email, messaging, chat rooms, collaborative platforms, social networking environments, and other forms of direct electronic communication when those technologies are used or discussed as part of the educational program.

Students will be taught not to share sensitive personal information with unknown or unauthorized individuals online.

Personal information may include, as appropriate:

- Full name;
- Home address;
- Personal telephone number;
- Passwords;
- Personal email addresses;
- Location information;
- Photographs or videos;
- Information about schedules or routines; and
- Other information that could reasonably identify or locate a student.

6. Unauthorized Access and Hacking

Students and other users may not attempt to gain unauthorized access to school networks, accounts, devices, systems, applications, or data.

Prohibited activities include, but are not limited to:

- Attempting to bypass internet filters or security controls;
- Using another person's account or credentials without authorization;
- Attempting to discover or obtain another user's password;
- Hacking or attempting to gain unauthorized system access;
- Introducing malicious software or code;
- Intentionally disrupting networks or technology services;
- Altering or deleting data without authorization; and
- Using school technology to engage in unlawful activity.

Suspected security incidents should be reported promptly to the School Administrator or designated technology personnel.

7. Protection of Student Personal Information

Heartwood Montessori will take reasonable measures to protect against the unauthorized disclosure, use, and dissemination of personal information regarding minors.

Students will receive age-appropriate instruction about protecting personal information online.

School personnel are expected to use student information only for authorized educational and operational purposes and in accordance with applicable school policies and privacy requirements.

8. Monitoring of Student Online Activities

As required by CIPA, Heartwood Montessori will provide for the monitoring of the online activities of minors when students access the internet through school-provided technology or networks.

Monitoring may include:

- Direct adult supervision;
- Review of student activity on school-managed devices or accounts;
- Internet filtering and network security tools;
- Device-management systems; and
- Other reasonable methods designed to promote student safety and appropriate technology use.

Monitoring will be implemented in a manner consistent with the School's educational mission and applicable privacy requirements.

Students should understand that use of school-owned devices, accounts, networks, and technology systems may be monitored and should not be considered private to the extent permitted by law and school policy.

9. Digital Citizenship and Online Behavior Education

Heartwood Montessori will educate students, at developmentally appropriate levels, about safe and responsible online behavior.

Instruction may include:

- Responsible and respectful digital communication;
- Appropriate interactions with others online;
- Online privacy and protection of personal information;
- Recognizing unsafe or inappropriate online situations;
- Evaluating online information and sources;
- Responsible use of digital content;
- Cyberbullying awareness;
- How to respond to and report cyberbullying;
- Seeking assistance from a trusted adult;
- Digital footprints and the consequences of online actions; and
- Responsible use of emerging technologies and digital tools.

For younger students, these concepts may be taught through simple, concrete expectations emphasizing asking an adult, protecting private information, using approved resources, kindness, and immediately reporting anything online that makes the child uncomfortable or concerned.

10. Cyberbullying

Heartwood Montessori does not permit the use of school technology or networks to harass, intimidate, threaten, humiliate, or otherwise harm another individual.

Students will be taught how to recognize cyberbullying and how to respond appropriately, including:

- Not participating in or forwarding harmful communications;
- Preserving information when appropriate so an adult can assist;
- Reporting concerning behavior to a guide, teacher, administrator, parent, or other trusted adult; and
- Seeking adult assistance rather than retaliating online.

Reports of cyberbullying involving the school community will be addressed according to applicable school policies.

11. Staff Responsibilities

School employees who supervise students using technology are responsible for supporting safe and appropriate technology use.

Staff should:

- Model responsible digital citizenship;
- Provide reasonable supervision of student technology use;
- Direct students toward developmentally appropriate resources;
- Reinforce internet safety expectations;
- Respond when students encounter inappropriate material;
- Report suspected cybersecurity or student safety concerns;
- Protect confidential student information; and
- Follow school procedures regarding approved applications, platforms, and technology resources.

12. Circumvention of Safety Measures

Users may not intentionally disable, bypass, defeat, or attempt to circumvent the School's internet filtering, monitoring, device-management, or cybersecurity systems.

Students who discover a method of bypassing a technology safeguard should report the issue to a staff member rather than attempting to use or share the method.

13. Artificial Intelligence and Emerging Technologies

When artificial intelligence or other emerging digital technologies are made available to students, their use must be developmentally appropriate, educationally purposeful, and consistent with School expectations.

Students should not enter personally identifiable, confidential, or sensitive information about themselves or others into an artificial intelligence system unless the School has specifically authorized that use.

The School may establish additional procedures regarding approved AI tools, student accounts, adult supervision, privacy, academic integrity, and age-appropriate use.

14. Violations

Violations of this policy may result in appropriate educational or disciplinary responses, including restriction or suspension of technology privileges.

The School will consider the student's age, developmental level, intent, circumstances, and seriousness of the behavior when determining an appropriate response.

Serious incidents involving safety, security, unlawful activity, or threats to individuals or school systems may be referred to the Head of School or other appropriate authorities.

15. No Technology Protection Measure Is Infallible

Heartwood Montessori recognizes that no filtering or monitoring technology can completely prevent access to all inappropriate content.

The School therefore combines technological safeguards with adult supervision, student education, clear expectations, and partnership with families.

Families are encouraged to reinforce responsible digital citizenship and internet safety practices at home.

16. Public Notice and Adoption

In accordance with applicable CIPA requirements, Heartwood Montessori will provide reasonable notice and conduct at least one public hearing or meeting regarding the proposed Internet Safety Policy and technology protection measures before adoption.

For purposes applicable to a private school, notice will be provided to the appropriate constituent group.

The School will maintain appropriate documentation of the policy's adoption and its implementation.

17. Administration and Review

The Head of School or designee is responsible for overseeing implementation of this policy, including:

- Maintaining appropriate internet filtering or technology protection measures;
- Establishing procedures for monitoring student internet activity;
- Supporting developmentally appropriate internet safety and digital citizenship education;
- Maintaining appropriate CIPA compliance documentation;
- Reviewing technology safeguards and practices as technology evolves; and
- Reviewing this policy periodically and recommending revisions when appropriate.

CIPA Compliance Statement

Heartwood Montessori intends to maintain and enforce an Internet Safety Policy and technology protection measures consistent with the requirements of the Children's Internet Protection Act.

The School's internet safety program addresses:

1. Access by minors to inappropriate matter on the internet and World Wide Web;
2. The safety and security of minors when using email, chat rooms, and other forms of direct electronic communication;
3. Unauthorized access, including hacking and other unlawful online activities;
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors;
5. Measures designed to restrict minors' access to materials harmful to minors;
6. Monitoring of the online activities of minors; and
7. Education of minors regarding appropriate online behavior, including interaction with others through social networking and chat environments and cyberbullying awareness and response.

Adopted by: _____

Date of Public Notice: _____

Date of Public Hearing/Meeting: _____

Date Adopted: _____

Signature: _____

Title: _____

Student Technology Use Policy (Staff)

Staff Implementation & Procedures

Applies To: All staff supervising or supporting student technology use

Related Policy: Children's Internet Protection Act (CIPA) Internet Safety Policy

Responsible Administrator: Head of School / School Administrator

Review Cycle: Annual

Effective Date: _____

1. Purpose

Technology at Heartwood Montessori is a **tool for learning, not an end in itself**. Its use should be intentional, developmentally appropriate, and consistent with Montessori principles of independence, concentration, purposeful work, responsibility, and respect.

This procedure provides staff with clear expectations for implementing the School's CIPA Internet Safety Policy and supervising student use of computers, tablets, internet resources, applications, digital communication, and other technology.

2. Guiding Principle: Purpose Before Technology

Before introducing technology, staff should consider:

Does this technology meaningfully support the child's learning?

Technology should generally be used when it:

- Supports a defined educational purpose;
- Extends or enriches classroom learning;
- Provides access to appropriate research or information;
- Supports creativity, communication, or skill development;
- Provides an appropriate accommodation or learning support; or
- Develops responsible digital literacy.

Technology should not routinely replace hands-on materials, meaningful human interaction, movement, outdoor experiences, or developmentally appropriate concrete learning.

3. Staff Responsibilities

When students use school technology or access the internet at school, staff are expected to:

- Provide developmentally appropriate supervision;
- Clearly communicate the purpose of the technology activity;
- Direct students to approved websites, applications, and resources when appropriate;
- Reinforce safe and respectful online behavior;
- Protect student privacy and confidential information;
- Monitor student online activity consistent with the School's CIPA Internet Safety Policy;
- Intervene when technology is being used inappropriately;
- Report concerning content, communications, or security issues; and
- Model healthy, responsible, and respectful technology use.

Internet filtering does not replace active adult supervision.

4. Student Expectations

Staff should teach and consistently reinforce these simple expectations:

Use technology with purpose.

Use school technology for the learning activity or purpose approved by a staff member.

Protect privacy.

Do not share passwords, addresses, phone numbers, personal schedules, locations, or other private information without permission.

Be kind and respectful.

Digital communication should reflect the same expectations for grace, courtesy, and respect that apply to face-to-face interactions.

Use only your own account.

Students may not access another person's account, files, or information without authorization.

Stay within approved spaces.

Students should use websites, applications, accounts, and resources appropriate to the activity.

Do not bypass safeguards.

Students may not attempt to disable or circumvent internet filters, device restrictions, security controls, or monitoring systems.

Ask when unsure.

If a student is uncertain whether a website, message, download, application, or activity is appropriate, the student should ask a staff member.

Tell an adult.

Students should immediately tell a trusted adult if they encounter content or communication that is inappropriate, frightening, threatening, unsafe, or makes them uncomfortable.

5. Before Students Use Technology

Staff should:

- Identify the educational purpose;
- Select an appropriate device, application, website, or digital resource;
- Consider the age and developmental readiness of the students;
- Confirm that students understand the expectations for the activity;
- Consider whether students will enter or share personal information;
- Provide an appropriate level of adult supervision; and
- Use school-approved accounts, applications, and platforms whenever required.

For younger students, staff should favor teacher-selected resources and direct supervision rather than unrestricted internet searching.

6. During Technology Use

Staff should remain reasonably aware of what students are doing online.

Depending on student age and activity, appropriate supervision may include:

- Circulating through the classroom;
- Positioning screens so they are reasonably visible;
- Checking student work periodically;
- Using classroom or device-management tools;
- Reviewing browsing or account activity when appropriate;
- Conducting research alongside younger students; and
- Redirecting students promptly when technology use becomes unrelated to the learning purpose.

The level of independence may increase as students demonstrate maturity, responsibility, and appropriate digital citizenship.

7. If a Student Encounters Inappropriate Content

If inappropriate material appears accidentally:

1. **Direct the student away from the content.**
2. **Respond calmly.** Avoid making the student feel that accidental exposure itself is misconduct.
3. **Determine generally what occurred** without unnecessarily displaying or circulating the material.

4. **Document or preserve relevant information** when needed for follow-up, while avoiding unnecessary copies of inappropriate content.
5. **Notify the appropriate administrator or technology contact** if filtering, security, or student safety requires attention.
6. **Follow applicable reporting and student-safety procedures** when the content raises a safeguarding concern.

Staff should not ask students to repeatedly reopen inappropriate content merely to demonstrate what they encountered.

8. Student Misuse of Technology

When technology is intentionally misused, staff should respond in a manner that is educational, proportionate, and developmentally appropriate.

Possible responses include:

- Conversation and redirection;
- Review of the applicable technology expectation;
- Temporary restriction of technology privileges;
- Increased supervision;
- Restorative action when another person was affected;
- Communication with the student's family;
- Referral to school administration; or
- Other action under applicable School policies.

Serious concerns—including threats, cyberbullying, attempts to compromise school systems, intentional access to significantly inappropriate material, or suspected unlawful activity—should be promptly referred to administration.

9. Student Privacy and Personal Information

Staff should help students understand that protecting personal information is part of responsible technology use.

Students should not be directed to provide unnecessary personal information to websites, applications, AI systems, or other online services.

Staff should use school-approved systems when handling student information and follow School privacy and confidentiality requirements.

Photographs, recordings, student work, names, and other identifying student information should only be shared in accordance with School policies and applicable permissions.

10. Artificial Intelligence

When AI tools are used with students, staff should ensure that use is:

- Developmentally appropriate;
- Connected to a legitimate educational purpose;
- Consistent with School expectations;
- Appropriately supervised; and
- Protective of student privacy.

Students should not enter confidential, sensitive, or personally identifiable information about themselves, classmates, families, or staff into AI tools unless specifically authorized.

Staff should help students understand that AI-generated information can be inaccurate and should be evaluated rather than automatically accepted as fact.

AI should support learning and thinking—not replace the student's own thinking, creativity, effort, or demonstration of understanding.

11. Digital Citizenship

Internet safety education should be integrated naturally into the educational environment rather than treated solely as a technology rule.

Developmentally appropriate topics may include:

- Protecting private information;
- Asking permission before sharing;
- Respectful online communication;
- Recognizing advertising and unreliable information;
- Evaluating sources;
- Digital footprints;
- Copyright and responsible use of others' work;
- Cyberbullying awareness and response;
- Recognizing suspicious links or messages;
- Seeking help from a trusted adult; and
- Healthy boundaries around technology use.

12. Family Partnership

Staff should communicate significant technology concerns to families when appropriate.

Families should be encouraged to reinforce similar expectations regarding:

- Privacy;
- Respectful communication;
- Appropriate content;
- Responsible device use;

- Digital citizenship; and
- Seeking adult help when something online feels unsafe.

Consistent expectations between home and school help children develop responsible technology habits.

13. Staff Quick-Response Procedure

When a technology concern occurs, staff can use:

STOP → SUPPORT → SECURE → SHARE

STOP

Stop or redirect inappropriate or unsafe technology use.

SUPPORT

Attend to the student and determine whether there is an immediate safety or well-being concern.

SECURE

Protect accounts, devices, evidence, and personal information as appropriate. Do not unnecessarily forward or reproduce inappropriate material.

SHARE

Report the concern to the appropriate administrator or technology contact when follow-up is necessary.

14. Staff Pre-Use Check

Before student technology use, ask:

- Is there a clear educational purpose?
- Is the technology developmentally appropriate?
- Am I comfortable with the level of supervision?
- Are students using an approved resource or platform when required?
- Have students been given clear expectations?
- Is student personal information protected?
- Do students know what to do if something inappropriate appears?
- Does technology add meaningful value compared with a hands-on alternative?

15. Relationship to the CIPA Internet Safety Policy

This procedure supports implementation of Heartwood Montessori's **CIPA Internet Safety Policy**.

The CIPA policy establishes the School's overall requirements regarding internet filtering, monitoring, internet safety, inappropriate material, unauthorized access, student privacy, digital citizenship, and cyberbullying.

This document translates those requirements into **everyday staff practices**.

When there is a conflict between this procedure and the CIPA Internet Safety Policy, the CIPA Internet Safety Policy controls.

Our Shared Standard

Technology should serve the child—not the other way around.

Our goal is not simply to restrict inappropriate technology use. Our goal is to help children gradually develop the independence, judgment, responsibility, and digital citizenship necessary to use technology thoughtfully, safely, and purposefully.