

CHILD SAFETY / AGES 10 TO 18 / IN PERSON, VIRTUAL, AI ENABLED

IIAI FOUNDATION, INC.

Child Safety and Safeguarding Policy

INTERNATIONAL INSTITUTE OF AI INFLUENCE / ATLANTA, GEORGIA / CPD PROVIDER NO. 50846

Organization	IIAI Foundation, Inc. (International Institute of AI Influence), a Georgia nonprofit corporation and 501(c)(3) public charity
Principal office	1650 Marietta Blvd NW, Ste D58, Atlanta, GA 30318
Applies to	All programs serving participants under the age of 18, including AI Kids Korner and the Explorers, Creators, and Career Ready tiers
Policy owner	Designated Safeguarding Lead, reporting to the Board of Directors
Approved by	Board of Directors, IIAI Foundation, Inc., by resolution dated August 5, 2026
Version	Version 1.0
Effective date	August 5, 2026
Next scheduled review	August 5, 2027

1. Policy Statement

IIAI Foundation, Inc. is committed to the safety, dignity, and wellbeing of every child who participates in its programs. The Foundation has zero tolerance for abuse, exploitation, neglect, harassment, or the misuse of a child's image, voice, likeness, or personal data.

This policy establishes binding standards of conduct, screening, supervision, technology use, reporting, and response. Compliance is a condition of employment, contract, volunteer service, and board membership. Violations result in disciplinary action up to and including immediate removal, termination of contract, and referral to law enforcement.

Because the Foundation delivers artificial intelligence education, this policy carries specific obligations governing the use of AI tools with and about minors. These obligations are set out in Section 8 and apply in addition to, not in place of, all other provisions.

2. Scope and Definitions

2.1 Who is covered

This policy applies to all Covered Persons, defined as employees, officers, directors, instructors, teaching assistants, contractors, consultants, vendors with participant contact, interns, volunteers, and any adult acting on behalf of the Foundation in a program setting.

2.2 Where it applies

- Foundation facilities and any leased, borrowed, or partner site
- Off-site activities, field trips, community events, and partner schools
- Virtual instruction, webinars, recorded sessions, and asynchronous coursework
- All Foundation-owned digital channels, learning platforms, group chats, and AI tools used in programming
- Any contact between a Covered Person and a program participant that arises from the participant's involvement in a Foundation program, including contact outside program hours

2.3 Key definitions

- Child or minor: any person under 18 years of age.
- Abuse: physical abuse, sexual abuse or exploitation, emotional or psychological abuse, and neglect, as those terms are used in O.C.G.A. Section 19-7-5 and related Georgia law.
- Grooming: any pattern of behavior intended to build trust with a child or a child's caregiver for the purpose of future abuse or exploitation, including secrecy, gift-giving, isolation, and boundary testing.
- Synthetic likeness: any AI-generated or AI-modified image, video, audio, avatar, or digital twin that depicts or imitates an identifiable person.
- Designated Safeguarding Lead (DSL): the named officer responsible for receiving reports, coordinating response, and maintaining safeguarding records. The Board appoints the DSL and at least one Deputy DSL.

3. Governance and Accountability

1. The Board of Directors holds ultimate responsibility for child safety and reviews safeguarding performance at least annually.
2. The Designated Safeguarding Lead administers this policy day to day, receives all reports, maintains the safeguarding log, and advises leadership.

3. A Deputy Designated Safeguarding Lead acts whenever the DSL is unavailable or is the subject of a report.
4. The Board Director for compliance and operations conducts an annual audit of screening records, training completion, consent files, and incident handling, and reports findings to the full Board.
5. No individual may serve as DSL who has a supervisory conflict that would prevent independent handling of a report. Reports concerning the President and CEO go directly to the Board Chair and to the Treasurer.

Contact for safeguarding matters: admin@iiaifoundation.org, marked SAFEGUARDING, and by telephone to the DSL at the number posted at each program site.

4. Screening, Selection, and Vetting

No adult may have contact with minors in a Foundation program before screening is complete and documented.

4.1 Required for every Covered Person with minor contact

- Written application and signed disclosure of any prior conviction, pending charge, or substantiated finding involving a minor
- Criminal background check, including a national criminal database search, county-level searches for all counties of residence in the prior seven years, and a national sex offender registry search
- Identity verification
- Minimum of two reference checks, at least one from a prior role involving minors where applicable
- Signed acknowledgment of this policy and of the Code of Conduct in Section 5
- Completion of child safety training before first participant contact

4.2 Disqualifying findings

Any conviction, plea, or substantiated administrative finding involving sexual offenses, offenses against a minor, child pornography or child sexual abuse material, kidnapping, violent felony, or the production or distribution of non-consensual intimate imagery is an absolute bar to any role with minor contact. Other findings are assessed case by case in writing by the DSL and one officer, with the assessment retained in the personnel file.

4.3 Ongoing

- Background checks are re-run at least every three years, and immediately upon receipt of credible adverse information
- Every Covered Person has a continuing duty to disclose any new arrest, charge, conviction, or protective order involving a minor within three business days
- Partner organizations that supply instructors or volunteers must certify in writing that their personnel meet screening standards equal to or stronger than this section

5. Code of Conduct

5.1 Required behavior

- Treat every participant with respect regardless of race, sex, disability, national origin, religion, or family circumstance
- Remain in view of another adult or in an open, observable space at all times when minors are present
- Use only Foundation-issued accounts, channels, and platforms for all participant communication
- Copy a parent or guardian, or a second Foundation adult, on any individual written communication with a minor
- Report any concern, disclosure, boundary violation, or policy breach immediately under Section 12
- Correct and document any accidental one-to-one situation as soon as it occurs

5.2 Prohibited behavior

The following are prohibited without exception:

- Being alone with a minor who is not your own child, whether in person, by phone, by video, or by private message
- Private or unmonitored electronic contact of any kind, including personal phone numbers, personal email, direct messages, disappearing-message apps, and personal social media connections or follows
- Transporting a minor alone in a vehicle
- Any sexual conduct, sexualized language, sexual jokes, or discussion of a Covered Person's or a minor's sexual activity
- Romantic or dating contact with any participant under 18, regardless of the age of consent
- Sharing or displaying sexually explicit, violent, or otherwise age-inappropriate material
- Physical discipline, restraint except to prevent imminent injury, isolation as punishment, humiliation, threats, or verbal abuse
- Physical contact beyond brief, public, non-sexual contact appropriate to the setting, and only where welcomed by the child
- Giving gifts, money, or special privileges to an individual minor
- Asking a minor to keep any secret from a parent, guardian, or Foundation staff
- Possessing, using, or being under the influence of alcohol, cannabis, or illegal drugs during programming, or using tobacco or vape products in the presence of minors
- Possessing a weapon at any program site or activity
- Photographing or recording a minor on a personal device
- Meeting a participant outside of Foundation programming without the written consent of the parent or guardian and prior written notice to the DSL

6. Supervision Standards for In-Person Programming

- Two-adult rule: a minimum of two screened adults are present for every activity involving minors. A single adult is never left in sole charge.
- Ratios: at least one screened adult for every ten participants ages 10 to 12, and one for every fifteen participants ages 13 to 18, with a minimum of two adults regardless of group size.
- Open environment: doors remain open or have unobstructed interior windows. Interior spaces are subject to unannounced walkthroughs by the DSL or a designee.
- Restrooms: adults do not enter a single-occupancy restroom with a minor. For younger participants needing assistance, a second adult is notified and remains at the door.
- Sign in and out: participants under 16 are released only to a parent, guardian, or person named in writing by the parent or guardian, with photo identification checked.
- Attendance: a written roster is kept for every session and retained under Section 15.
- Off-site activities: require advance written parental permission, a documented adult roster, emergency contact information on hand, and a first-aid trained adult present.
- Medical: a current emergency contact and medical authorization form is on file for each minor before participation. Emergency services are called for any suspected serious injury, and the parent or guardian is notified without delay.

7. Virtual and Online Program Safeguards

- All virtual sessions use Foundation-managed accounts on approved platforms with waiting rooms enabled, host-controlled admission, and locked meetings after the start.
- Two screened adults are present in every virtual session with minors, one facilitating and one monitoring chat and participants.
- Private one-to-one chat between an adult and a minor is disabled. Direct messaging between adults and minors on any Foundation platform is disabled.
- Breakout rooms containing minors are monitored by a screened adult and are never one adult with one minor.
- Screen sharing is restricted to hosts and co-hosts. Participant annotation and file transfer are disabled by default.
- Recording occurs only with prior written parental consent, is announced at the start of the session, is stored on Foundation-controlled storage with access restricted to authorized staff, and is deleted per Section 15.
- Learning platform accounts for minors are created and administered by the Foundation. Minors do not create their own program accounts and do not supply their own credentials to third-party services.
- Content filtering and safe-search are enabled on all Foundation-managed devices and networks used by minors.

- Instructors do not conduct sessions from a private bedroom setting and use a neutral or virtual background.
- Devices loaned to participants under the AI Access and Tools program are configured with content filtering, managed accounts, and a written device agreement signed by the parent or guardian.

8. Artificial Intelligence Safeguards for Minors

These provisions govern the use of generative and analytical AI tools in any program serving minors. They apply to instructors, participants, and any content produced in or for programming.

8.1 Likeness, voice, and synthetic media

- The Foundation does not create, commission, or permit the creation of AI-generated avatars, digital twins, voice clones, face swaps, or any other synthetic likeness of a minor. Parental consent does not waive this prohibition.
- A minor's photograph, video, or voice recording is never uploaded to a generative AI service, used as a reference image or prompt input, or used to train, fine-tune, or condition any model.
- Participants are instructed not to upload images or recordings of themselves, classmates, family members, or any other identifiable person into AI tools during programming.
- Any AI-generated depiction of a person used in instruction is a fictional adult figure and is reviewed by the instructor before display.
- Instruction on synthetic media includes explicit teaching on consent, likeness rights, deepfake harm, and the illegality of producing sexualized imagery of minors.

8.2 Tool approval and age gating

- Only tools on the Foundation's Approved AI Tools List may be used with minors. The DSL and the technology director maintain the list and review it at least quarterly.
- Approval requires review of the tool's minimum age terms, data handling and training practices, content safety controls, and retention policy. A tool that trains on user input without an enterprise or education opt-out is not approved for use with minors.
- Participants under 13: AI tools are operated by the instructor on a shared screen or through Foundation-managed accounts. Participants under 13 do not hold individual accounts on third-party AI services.
- Participants 13 to 17: individual use is permitted only on approved tools, through Foundation-administered accounts, with documented parental consent, and under active supervision.
- Open-ended companion, roleplay, or character chatbots are not used in any program serving minors.

8.3 Prompt and output standards

- Prohibited prompts and outputs include sexual or suggestive content, content depicting minors in any sexualized manner, graphic violence, self-harm or suicide content, harassment or targeting of an identifiable person, instructions for weapons or dangerous substances, and content that demeans a protected group.
- Instructors review AI outputs before they are displayed to a group, shared beyond the classroom, or published.
- Participant prompt and output activity on Foundation-managed accounts is logged and subject to review. Participants and parents are told this in writing at enrollment.
- No AI output is published under a minor's name or with a minor's image without written parental consent and Foundation review.

8.4 Escalation when a tool produces harmful content

1. Stop the activity and remove the content from the shared display immediately.
2. Do not download, forward, print, or reproduce the material.
3. Preserve the account identifier, timestamp, tool name, and prompt history without copying the material itself.
4. Notify the DSL the same day. The DSL determines regulatory and law enforcement reporting obligations.
5. If the content is or may be child sexual abuse material, the DSL reports to the National Center for Missing and Exploited Children CyberTipline at report.cybertip.org or 1-800-843-5678, and to law enforcement. Reporting is mandatory and is not delayed for internal review.
6. Notify the affected participant's parent or guardian, and provide support resources.

8.5 Data minimization in AI use

- Participant names, dates of birth, addresses, school names, contact details, photographs, and any other personal identifier are never entered into a third-party AI tool.
- Instructional examples use fictional or de-identified data.
- Assessment and portfolio artifacts are stored on Foundation-controlled systems, not in third-party AI tool histories.

9. Photography, Media, and Likeness

- Photography and recording of minors occur only on Foundation-issued devices, by designated staff, in program settings, and only where written parental consent is on file.
- Consent is granular. Parents may consent to internal program use, to grant reporting and funder materials, and to public marketing separately, and may withdraw consent at any time in writing.

- Published images do not include a minor's full name, school, home location, or contact information. First name only is used where a name is needed.
- Images of minors are stored on Foundation-controlled storage with restricted access and are deleted per Section 15.
- Images of minors are never used as inputs to AI generation, editing, or enhancement tools, consistent with Section 8.1.
- No minor is required to be photographed or recorded as a condition of participation.

10. Data Protection and Children's Privacy

- The Foundation collects the minimum personal information necessary to operate its programs, safeguard participants, and meet funder reporting requirements.
- For participants under 13, the Foundation obtains verifiable parental consent before collecting personal information online, provides a direct notice describing what is collected and how it is used, and obtains separate consent before any disclosure of that information to a third party, consistent with the Children's Online Privacy Protection Rule as amended, which took full effect on April 22, 2026.
- Parents and guardians may review, correct, or request deletion of their child's personal information, and may refuse further collection, by writing to admin@iiaifoundation.org.
- Children's personal information is retained only as long as reasonably necessary for the purpose for which it was collected, then securely deleted.
- Access to participant records is role-restricted, accounts require multifactor authentication, and devices holding participant data are encrypted.
- Participant data is not sold, rented, or used for targeted advertising, and is not shared with third parties except as necessary to deliver the program, as required by law, or as separately consented to.
- Vendors handling participant data sign a written agreement addressing confidentiality, security, permitted use, prohibition on training models with participant data, and breach notification.
- Suspected data breaches involving participant information are reported to the DSL within 24 hours and handled under the Foundation's incident response procedure.

11. Recognizing Concerns

Covered Persons are not expected to investigate or to reach a conclusion. They are expected to notice and report.

11.1 Signs that may indicate harm

- Unexplained injuries, injuries inconsistent with the explanation given, or repeated injuries
- Marked change in behavior, withdrawal, regression, fearfulness, or aggression
- Age-inappropriate sexual knowledge or behavior

- Persistent hunger, poor hygiene, untreated medical needs, or inadequate clothing
- Fear of a particular adult or reluctance to go home
- Disclosure by the child, by a sibling, or by another participant

11.2 Signs of grooming by an adult

- Seeking time alone with a particular child or engineering one-to-one situations
- Private communication outside Foundation channels
- Gifts, favors, or special attention to one child
- Requests for secrecy or discouraging the child from telling a parent
- Excessive physical contact, or contact that continues after the child pulls away
- Contact with the child or the family outside program purposes without notice to the Foundation

11.3 If a child discloses

1. Listen. Stay calm. Do not react with shock, anger, or disbelief.
2. Do not ask leading questions. Use open prompts such as "tell me more about that."
3. Do not promise confidentiality. Say that you must tell someone whose job it is to help keep them safe.
4. Do not investigate, confront the alleged abuser, or contact the alleged abuser.
5. Write down what the child said in the child's own words, with the date, time, and setting, as soon as possible.
6. Report the same day under Section 12.

12. Reporting Obligations

12.1 External reporting is mandatory

Personnel of an organization that provides education, training, or care to children are mandated reporters under O.C.G.A. Section 19-7-5. Any Covered Person who has reasonable cause to believe that a child has been abused must make a report immediately, and in no case later than 24 hours from the time reasonable cause arises.

The Foundation requires all Covered Persons, whether or not individually classified as mandated reporters, to report on the same standard and timeline.

Immediate danger	Call 911
Georgia DFCS Child Protective Services	1-855-GA-CHILD (1-855-422-4453), available 24 hours a day
Child sexual abuse material or online exploitation	NCMEC CyberTipline at report.cybertip.org or 1-800-843-5678

Internal notification	Designated Safeguarding Lead, same day, in writing to admin@iiaifoundation.org marked SAFEGUARDING
------------------------------	--

- The duty to report to DFCS or law enforcement rests with the individual who has the reasonable cause. Telling a supervisor does not discharge it. Internal notification is required in addition, not instead.
- No Covered Person may be instructed, pressured, or permitted to delay or withhold an external report pending internal review.
- Knowingly and willfully failing to report as required is a criminal offense in Georgia and is grounds for immediate termination.
- Reports made in good faith carry statutory immunity from civil and criminal liability.

12.2 Internal reporting of policy violations

Any breach of this policy, including boundary violations that do not rise to suspected abuse, is reported to the DSL within 24 hours. Concerns may be raised by staff, volunteers, participants, parents, or partner organizations. Anonymous reports are accepted and investigated to the extent the information allows.

13. Response to Allegations Against a Covered Person

1. The DSL logs the report on receipt and confirms that any required external report has been made. If it has not, the DSL makes it immediately.
2. The subject of the allegation is removed from all contact with minors pending resolution. Removal is a neutral protective step and is not a finding.
3. The Foundation does not conduct its own investigation into suspected criminal conduct and does not interview the child. It cooperates fully with DFCS and law enforcement and follows their direction on sequencing and communication.
4. The parent or guardian of any affected child is notified promptly unless law enforcement or DFCS directs otherwise.
5. The Board Chair is notified within 24 hours of any allegation involving suspected abuse. The Foundation's insurer and counsel are notified as required.
6. Evidence, records, logs, and communications relevant to the matter are preserved and are not altered or deleted.
7. On conclusion, the DSL documents the outcome, any disciplinary action, and any corrective change to practice, and reports to the Board.
8. Substantiated findings result in termination and referral to relevant authorities and licensing or registry bodies where applicable.

14. Non-Retaliation and Confidentiality

- The Foundation prohibits retaliation against any person who reports a concern in good faith, who participates in an inquiry, or who refuses to participate in conduct that violates this policy.
- Retaliation is itself a violation of this policy and results in disciplinary action up to termination.
- A report made in good faith that is not substantiated does not expose the reporter to discipline. Knowingly false reports made in bad faith do.
- Information about a report is shared only with those who need it to protect the child, to comply with law, or to conduct the response. The identity of the reporting person is protected to the extent the law allows.

15. Training and Recordkeeping

15.1 Training

- Every Covered Person completes child safety and mandated reporter training before first contact with minors, and refresher training annually.
- Training covers this policy, recognizing abuse and grooming, responding to disclosure, mandated reporting duties under Georgia law, the AI safeguards in Section 8, and virtual program conduct.
- Board members complete an annual safeguarding governance briefing.
- Participants receive age-appropriate instruction on personal boundaries, online safety, AI-specific risks including deepfakes and manipulated media, and how to raise a concern.
- Parents and guardians receive a plain-language summary of this policy at enrollment.

15.2 Records and retention

- Screening records, signed acknowledgments, and training completion are retained for the duration of service plus seven years.
- Safeguarding reports, incident records, and response documentation are retained permanently in a restricted-access file held by the DSL.
- Attendance rosters and supervision records are retained for three years.
- Media consent forms are retained for as long as the material is in use, plus three years.
- Session recordings involving minors are deleted within 90 days unless a documented instructional or legal reason requires longer retention.
- Participant personal information is deleted when no longer reasonably necessary, subject to any legal hold.

16. Adoption, Review, and Amendment

- This policy is adopted by resolution of the Board of Directors and takes effect August 5, 2026.

- The DSL reviews the policy no later than August 5, 2027, and after any significant incident, regulatory change, or change in program delivery or AI tooling.
- Amendments require Board approval. The current version is distributed to all Covered Persons and made available to parents and guardians on request.
- This policy supplements and does not limit any obligation imposed by law, funder agreement, or partner site policy. Where standards differ, the stricter standard applies.

Appendix A. Quick Reference: Reporting

A child is in immediate danger	Call 911. Then notify the DSL.
You suspect abuse or neglect	Report to DFCS at 1-855-422-4453 immediately, no later than 24 hours. Then notify the DSL in writing the same day.
A child discloses to you	Listen, do not question, do not promise secrecy, write it down, report as above.
You witness a boundary or policy violation	Notify the DSL within 24 hours in writing.
An AI tool produces harmful content	Stop, do not save or share, preserve context, notify the DSL the same day.
Suspected child sexual abuse material	Do not download or forward. Report to NCMEC at report.cybertip.org or 1-800-843-5678 and to law enforcement. Notify the DSL.
Suspected data breach involving a minor	Notify the DSL within 24 hours.

Post this page at every program site and include it in every virtual instructor briefing.

Appendix B. Acknowledgment and Agreement

To be signed before any contact with minors and retained in the personnel file.

I have received, read, and understand the IIAll Foundation, Inc. Child Safety and Safeguarding Policy. I agree to abide by the Code of Conduct in Section 5 and by all other provisions of the policy.

I understand that I am required to report suspected child abuse immediately and no later than 24 hours to the Georgia Division of Family and Children Services or to law enforcement, and to notify the Designated Safeguarding Lead, and that telling a supervisor does not satisfy this duty.

I understand the artificial intelligence safeguards in Section 8, including the prohibition on creating any synthetic likeness of a minor and on entering a minor's image, voice, or personal information into any AI tool.

I confirm that I have disclosed any conviction, pending charge, or substantiated finding involving a minor, and I agree to disclose any future arrest, charge, conviction, or protective order involving a minor within three business days.

I understand that violation of this policy may result in removal from my role, termination, and referral to law enforcement.

Printed name: _____

Role: _____

Signature: _____

Date: _____

Received by (Designated Safeguarding Lead): _____

Appendix C. Safeguarding Incident Record

Completed by the person raising the concern. Submit to the Designated Safeguarding Lead the same day. Record facts only. Do not include opinion or conclusions.

Date and time of report	
Person completing this form	
Role	
Child or children involved (name, age)	
Date, time, and location of the incident or concern	
Others present	
What was seen, heard, or disclosed (use the child's own words where applicable)	
Any visible injury or physical sign observed	
Immediate action taken	
External report made (agency, time, reference number)	
Parent or guardian notified (by whom, when)	
Signature and date	

For DSL use: date received, action taken, outcome, Board notification, review date.