Simeio researching & confronting the far right

Child Protection Policy

Version	Review date	Reviewed by	Key changes / summary	Next review due
v.1.0	10/9/2025	Program Coordinator	Initial drafting	
v.2.0	28/7/2026	CPFP & Director	Adoption for CERV grant with major additions and clarifications	July 2027

Table of Contents

1. Policy Purpose, Scope, Principles, and Public Access

1.1 Organizational commitment and scope

1.2 Fundamental safeguarding principles

1.3 Public availability, web access, and transparency

2. Definitions and Context-Specific Safeguarding Risks

2.1 Standard safeguarding definitions

2.2 Operational context and risk analysis for Simeio

3. Code of Conduct and Behavioral Guidelines

3.1 Key behavioral standards

3.2 Physical and digital boundary rules

4. Safe Recruitment and Vetting Procedures

4.1 Scope and mandatory application

4.2 Background vetting and screening standards

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 1/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 1/23

4.3 Onboarding and policy awareness

5. Data Protection, Media Protocols, and GDPR Compliance

5.1 Legal basis and scope

5.2 Informed consent and child assent framework

5.3 Handling children's research data, personal data, and case records

5.4 Media protocols (photos, videos, and audio recordings)

5.5 Data retention and disposal

5.6 Transparent privacy information

6. Safeguarding Orientation and Capacity Building

6.1 Proportional training model

6.2 Mandatory external e-learning requirements

6.3 Certificates of completion & administrative verification

7. Child Protection Focal Person, Policy Review, Incident Reporting, and Complaints Mechanism

7.1 Appointment and role of the Child Protection Focal Person

7.2 Policy revision cycle and monitoring

7.3 Incident reporting and escalation procedure

7.4 Complaints, feedback, and whistleblowing mechanism

Annex A: Code of Conduct Declaration Form

Annex B: Parental Consent & Child Assent Form Template

Annex C: Standard Privacy Notice (GDPR)

Annex D: Incident Report Form

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 2/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 2/23

1. Policy Purpose, Scope, Principles, and Public Access

1.1 Organizational commitment and scope

Zero-tolerance commitment: Simeio is fully committed to creating a safe, respectful, and protective environment for all children and youth (under 18 years of age) participating in its initiatives. Simeio maintains a zero-tolerance policy towards child abuse, violence, exploitation, discrimination, emotional distress, or neglect.

Human rights framework: This policy operates in accordance with the UN Convention on the Rights of the Child (UNCRC), the EU Charter of Fundamental Rights, EU CERV safeguarding standards, and applicable Greek child protection legislation.

Scope and applicability: This policy is binding on:

- All Simeio personnel (board members, executive management, employees, interns, and volunteers).
- External consultants, workshop facilitators, freelancers, and project partner staff.
- Any visitor, researcher, or third party attending or observing Simeio's activities.

Operational setting: This policy applies to all physical activity venues, digital platforms (online webinars, video calls, social media platforms), communication channels, and project interventions managed or co-managed by Simeio.

1.2 Fundamental safeguarding principles

Simeio's child protection practices are governed by five non-negotiable principles:

Best interests of the child: The safety, well-being, and rights of the minor are the primary consideration in every project design, risk assessment, and administrative decision.

Non-discrimination and equal protection: Every child has an equal right to protection without distinction of race, nationality, gender identity, religion, sexual orientation, disability, socio-economic background, or legal status.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 3/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 3/23

Do no harm and proactive risk prevention: All activities involving youth must undergo prior risk identification to prevent physical, psychological, or digital risk before execution.

Child participation and empowerment: Children are recognized as active rights-holders. They must be informed of their rights in plain, age-appropriate language and given safe channels to express their views freely.

Confidentiality and data protection: All records, personal details, and incident disclosures concerning minors are handled with strict confidentiality under EU GDPR standards.

1.3 Public availability, web access, and transparency

To ensure complete transparency and accountability to children, families, partners, and the general public:

Public online hosting: This Child Protection Policy is permanently published and publicly accessible on Simeio's official website at https://simeio.org.gr/child-protection-policy prior to the launch of any project activities involving minors.

Pre-activity distribution: A direct hyperlink to the online policy is systematically included in all workshop invitation materials, participant registration forms, parental consent packages, and partner agreement documents before any minor participates in Simeio's activities.

Open accessibility: The policy is maintained in an accessible, downloadable digital format (PDF) to ensure children, parents, caregivers, funding bodies, and external stakeholders can review it at any time.

2. Definitions and Context-Specific Safeguarding Risks

2.1 Standard safeguarding definitions

Child / Minor: Any human being under the age of eighteen (18) years, in accordance with the UN Convention on the Rights of the Child.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 4/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 4/23

Physical abuse: Any intentional or reckless application of physical force that results in, or has high potential to cause, physical injury, pain, or impairment to a child.

Emotional / psychological abuse: Any persistent pattern of behavior, verbal communication, threats, rejection, humiliation, isolation, or manipulation that degrades a child's self-worth, emotional stability, or developmental well-being.

Sexual abuse & exploitation: Any involvement of a child in sexual activity, contact, explicit communication, or exposure to sexual material, regardless of whether the child appears to consent or understand.

Neglect: The persistent failure to provide a child with adequate food, shelter, safety, supervision, medical care, or emotional support needed for their healthy development.

Exploitation: The act of taking unfair advantage of a child for labor, academic gain, organizational visibility, financial profit, or political leverage.

2.2 Operational context and risk analysis for Simeio

While Simeio's standard operations do not typically involve direct contact with minors, specific project activities under EU-funded programs—specifically educational workshops, seminars, public youth events, and digital learning sessions—may involve interaction with children.

To prevent harm, Simeio identifies and mitigates three main risk areas:

1. **In-Person workshops & events:** Risks include unmonitored access by external venue visitors, boundary violations during group dynamics, and unsupervised breaks or transit times.
2. **Public events & venues:** Risks include crowded venue safety hazards, unmonitored entry/exit times, and unauthorized photography or filming of minors.
3. **Digital platforms & webinars:** Risks include unmoderated chat rooms, cyberbullying, unsolicited private messages (DMs) to minors, and unauthorized screenshots or recording of video feeds.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 5/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 5/23

3. Code of Conduct and Behavioral Guidelines

This code of conduct establishes mandatory standards of behavior for all individuals working with or on behalf of Simeio. The fundamental ethical principles apply universally to both **Tier 1** (staff, facilitators, and volunteers in direct contact with minors) and **Tier 2** (administrative staff, external contractors, and observers without direct contact). While Tier 1 personnel bear direct operational responsibility for maintaining active supervision and boundary rules during live activities, Tier 2 personnel remain fully bound by all zero-tolerance policies and reporting obligations.

3.1 Key behavioral standards

All Simeio personnel and associated third parties must adhere to clear behavioral boundaries when participating in or observing project activities.

Mandatory expectations (DOs):

- **Respect and dignity:** Treat every minor with equity, respect, and dignity, regardless of background, identity, or ability.
- **Visible and open interactions:** Ensure that all interactions with children take place in open, visible, and well-supervised physical or digital settings.
- **Professional communication:** Use appropriate, encouraging, and age-appropriate language at all times.
- **Media consent:** Ensure valid parental/guardian consent is in place before capturing or publishing photos, video, or audio of any minor.
- **Immediate reporting:** Report any any incident, suspicion, or potential breach of this policy through established channels within 24 hours.

Strictly prohibited conduct (DON'Ts):

- **Violence and abuse:** Never engage in physical punishment, verbal degradation, emotional abuse, sexual harassment, or exploitation of any kind.
- **Isolated 1-on-1 contact:** Never spend unobserved, one-on-one time with a minor in isolated rooms, closed spaces, or private digital chat rooms.
- **Personal digital contact:** Never contact minors using personal social media accounts, personal phone numbers, or private direct messaging platforms.
- **Inappropriate physical touch:** Avoid unnecessary physical contact. Physical contact must always be non-intrusive, age-appropriate, and culturally sensitive.
- **Favors or gifts:** Never give personal gifts, money, or special favors to individual children outside established project framework rewards.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 6/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 6/23

3.2 Physical and digital boundary rules

To ensure safety across both in-person workshops and virtual interventions, personnel must follow specific boundary measures:

Physical environment safety:

- In-person workshops and youth events must always be facilitated by at least two adults (or one Tier 1 lead with active, open supervision by venue/coordinating staff).
- Adult personnel must use separate restroom facilities from minors whenever possible, or ensure youth facilities remain unmonitored by individual adults while in use.

Digital environment safety:

- Online webinars, digital workshops, and virtual sessions must be hosted via official Simeio accounts.
- Virtual workshops involving minors must have at least two adult co-hosts/moderators present in the session.
- Private chat functions between participants or between an adult host and an individual minor must be disabled during group webinars.
- Screen recording or capturing screenshots during digital sessions is strictly forbidden unless explicit parental consent and project authorization have been granted.

4. Safe Recruitment and Vetting Procedures

4.1 Scope and mandatory application

Simeio enforces rigorous “safer recruitment” standards to minimize the risk of appointing individuals who pose a threat to children. These procedures apply systematically to ALL categories of personnel prior to their engagement, including:

- Executive and administrative staff (full-time and part-time).
- Project managers, researchers, trainers, and facilitators.
- Volunteers, interns, and university trainees (πρακτικά ασκούμενοι).
- External consultants, freelancers, and contracted service providers.
- Staff deployed by partner organizations working on joint projects.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 7/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 7/23

4.2 Background vetting and screening standards

Simeio applies a risk-proportionate screening process based on the level of interaction with children:

Tier 1: Roles involving direct contact or direct access to children's data

Before facilitating workshops, webinars, or youth events involving minors, Tier 1 staff and volunteers MUST provide an official Clean Criminal Record Certificate (Πιστοποιητικό Λευκού Ποινικού Μητρώου) issued by the competent authority (e.g., via gov.gr for Greek residents) within the preceding six months prior to start of engagement.

Renewal: For long-term staff and regular direct-contact associates, this certificate must be reissued every two years.

Tier 2: Indirect or support roles (no contact with minors)

Administrative staff, finance personnel, IT developers, and general contractors are not subject to criminal background checks, self-declarations, or separate policy signatures. They are covered solely through a standard safeguarding clause included in their existing employment contract or service agreement, committing them to comply with Simeio's ethical principles.

Criteria for Automatic Disqualification

Any candidate—regardless of tier—who has a recorded conviction or pending prosecution for child abuse, neglect, sexual exploitation, domestic violence, human trafficking, or severe violent offenses is **strictly prohibited and permanently barred** from employment or engagement with Simeio.

4.3 Onboarding and policy awareness

Mandatory briefing: All personnel receive a copy of this policy upon joining and are briefed on their specific safeguarding obligations.

Pre-activity check-in: Prior to events involving minors, Tier 1 leads conduct a brief check-in with facilitators to review safety protocols and emergency steps.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 8/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 8/23

5. Data Protection, Media Protocols, and GDPR Compliance

5.1 Legal basis and scope

Simeio operates as a Data Controller in strict compliance with the EU General Data Protection Regulation (GDPR - Regulation EU 2016/679) and Greek Data Protection Legislation (Law 4624/2019).

Because children merit specific protection regarding their personal data, Simeio applies heightened safeguards across all data processing activities, including social research, educational workshops, public events, digital platforms, and case management records.

5.2 Informed consent and child assent framework

No personal data, research responses, photographs, or recordings of a minor MAY be collected or processed without prior written authorization obtained through the standard Parental Consent and Child Assent Form (Annex B) under the following dual framework:

- **Parental / Legal guardian consent:** Written, informed consent MUST be obtained from the child's parent or legal guardian prior to any activity involving data collection or media recording. Consent forms MUST specify the exact purpose, scope of processing, storage duration, and publication channels.
- **Child assent:** In addition to parental consent, the child's voluntary assent MUST be sought in an age-appropriate manner (verbal for younger children, written for youth aged 12+). A child's refusal to participate or be recorded MUST be respected at all times, regardless of parental consent.
- **Right to withdrawal:** Parents/guardians and children have the right to withdraw consent at any time without justification or negative consequences. Upon withdrawal, processing ceases immediately, and associated data/media MUST be deleted unless legally prohibited.

5.3 Handling children's research data, personal data, and case records

To safeguard minors during research, field interviews, and workshop activities, the following protocols MUST be implemented:

Data minimization: Simeio shall collect only the minimum necessary personal data required to achieve project objectives.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 9/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 9/23

Pseudonymization and anonymization: Direct identifiers (e.g., full name, address, phone number, school) MUST be separated from research responses and replaced with unique identification codes (e.g., Participant ID). Key files linking names to IDs MUST be stored in a separate, encrypted location.

Access control: Access to raw, unanonymized data or sensitive incident/case records is strictly restricted on a "need-to-know" basis to designated Tier 1 authorized personnel and the Child Protection Focal Person (CPFP).

Physical security: Hard copies of consent forms, research questionnaires, or incident reports MUST be kept in locked filing cabinets inside secured Simeio premises.

Digital Security: Digital files containing minors' data MUST be encrypted (using AES-256 or equivalent standard) and stored on secure cloud platforms or internal servers protected by multi-factor authentication (MFA) and strict access logs. Personal USB drives or unencrypted laptops MUST NOT be used to store unencrypted children's data.

5.4 Media protocols (photos, videos, and audio recordings)

When creating or publishing media featuring children:

- **Equipment and device usage (personal device protocol):**

Where official organization-owned capture devices are unavailable, staff and authorized associates MAY use personal smartphones or digital devices to capture photos, video, or audio of minors, provided the following strict safeguards are maintained:

1. **Device passcode protection:** Personal devices used for project capture MUST be secured with a strong PIN, password, or biometric lock (FaceID/Fingerprint).
2. **Prompt transfer and permanent local erasure:** All media files captured on personal devices MUST be uploaded to Simeio's secure, encrypted cloud folder within 24 hours (or by the end of the event day). Immediately after successful transfer, all files MUST be permanently deleted from the personal device, including clearing the device's "Recently Deleted" or trash folder.
3. **No personal cloud sync or sharing:** Captured media files MUST NOT be uploaded to personal cloud storage (e.g., personal iCloud, personal Google Photos), nor shared via personal social media, personal messaging apps (e.g., WhatsApp, Viber), or personal email accounts.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 10/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 10/23

- **Dignified representation:** Children MUST be portrayed in a respectful, dignified, and fully clothed manner. Images that portray children in vulnerable, distressed, or culturally inappropriate situations are strictly forbidden.
- **Anonymity in publication:** Public materials, website posts, social media content, or EU project reports MUST NOT combine a child's image with their full name, home address, school, or specific geographical location. Pseudonyms or first-name-only tags MUST be used.
- **Media transfer, storage, and device erasure:**

All photographs, video, and audio recordings featuring minors—whether captured on SD/memory cards or internal device storage—MUST be uploaded to Simeio's designated encrypted server/cloud drive within 24 hours of the event.

Immediately upon verifying that the upload is complete:

- **For camera memory cards:** SD cards MUST be formatted and wiped.
- **For mobile devices:** Local media files MUST be permanently deleted, including clearing the device's "Recently Deleted" or trash folder.
- **No secondary copies:** Media files MUST NOT be retained on personal drives, memory cards, or unencrypted local storage.

5.5 Data retention and disposal

Retention period: Personal data and project records pertaining to minors MUST be retained only for as long as required by the specific EU grant agreement (typically 3 to 5 years following formal project closure for auditing purposes).

Secure destruction: Upon expiration of the mandatory retention period:

- **Digital records** MUST be permanently deleted (e.g., through secure cloud deletion and emptying system trash on encrypted organizational devices) ensuring data cannot be recovered.
- **Physical documents** MUST be securely destroyed (e.g., manually torn into small, illegible pieces or shredded) to ensure that sensitive personal data cannot be reconstructed or read prior to disposal in standard waste.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 11/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 11/23

5.6 Transparent privacy information

Prior to any data collection, parents and children **MUST** be provided with a concise, transparent privacy document. Simeio utilizes the standardized template found in Annex C: Standard Privacy Notice (GDPR) for Minors' Data for all activities to ensure individuals are fully informed of their rights.

6. Safeguarding Orientation and Capacity Building

6.1 Proportional training model

Recognizing Simeio's small operational scale and project-specific engagement with children, safeguarding capacity building is fulfilled through recognized external, open-access digital training programs, rather than internal training delivery.

Training is mandatory for all staff, board members, facilitators, or volunteers prior to their direct involvement in any project, workshop, or research activity involving minors.

6.2 Mandatory external e-learning requirements

Pre-activity completion: Prior to implementing any activities involving children, designated team members MUST complete an accredited, self-paced online safeguarding module offered by a recognized international or European body (e.g., UNICEF, Council of Europe, Keeping Children Safe, or EU Academy).

Core competencies covered: The selected e-learning course must cover:

1. Basic principles of child protection and safe professional boundaries.
2. Recognizing signs of abuse, distress, or online risks.
3. Steps for receiving disclosures and initiating incident reporting.

6.3 Certificates of completion & administrative verification

Upon finishing the required online module, all involved individuals MUST submit a copy of their digital completion certificate. The CPFP briefly verifies that the certificate is authentic, current, and issued by a recognized body before saving a PDF copy to the project audit archive and recording it in the digital Training Log (a file containing names, roles, completion dates, course titles, and attached PDF certificates for all trained persons).

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 12/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 12/23

7. Child Protection Focal Person, Policy Review, Incident Reporting, and Complaints Mechanism

7.1 Appointment and role of the Child Protection Focal Person

Simeio designates one staff member to serve as the Child Protection Focal Person (CPFP). For all organizational operations and grant-funded activities involving minors, the designated CPFP is Ioanna Meitani, Program Coordinator, reachable at im@simeio.org.gr].

Key responsibilities of the CPFP include:

Internal oversight: Managing compliance by collecting signed Codes of Conduct (Annex A) from Tier 1 personnel prior to activity launch, while confirming that Tier 2 personnel and external contractors are covered by the mandatory safeguarding clause in their contracts.

Incident management: Receiving, documenting, and managing safeguarding concerns or disclosures according to the procedure set out in Section 8 and utilizing the Incident Report Form (Annex D).

Training and record keeping: Conducting administrative checks on external e-learning certificates (confirming completion dates and issuing bodies for all staff and external contractors) and maintaining the organizational training log.

Data protection liaison: Serving as the main contact for data protection inquiries or GDPR rights requests regarding children's data.

7.2 Policy revision cycle and monitoring

To keep this Child Protection Policy current, practical, and fully compliant with EU standards, Simeio enforces a structured review cycle:

Annual review: This policy is formally reviewed every twelve (12) months by Simeio leadership to account for operational changes, legislative updates, or new grant requirements.

Incident-triggered review: Following any reported safeguarding concern, breach, or audit recommendation, the CPFP will review operational procedures immediately and update the policy as needed.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 13/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 13/23

Implementation monitoring: Prior to launching activities involving minors, the CPFP verifies operational readiness—checking that consent forms, training logs, and codes of conduct are complete—using an internal Safeguarding Compliance Checklist.

7.3 Incident reporting and escalation procedure

Step 1: Internal reporting

- **Immediate response:** Anyone (staff, external contractor, partner, or participant) who receives a disclosure of abuse, observes unsafe behavior, or suspects a safeguarding risk MUST report it to the Child Protection Focal Person (CPFP) within 24 hours.
- **Child-centered approach:** When a child discloses information, personnel MUST listen calmly, reassure the child that they were right to speak up, and avoid making promises of absolute confidentiality (explaining that help must be brought in).

Step 2: Documentation

- **Factual recording:** The person receiving the report or disclosure **MUST** record the facts immediately using the Incident Report Form (Annex D) stating: date, time, location, involved parties, and exact words used, without adding personal opinions or assumptions.
- **Secure storage:** All incident logs and written reports MUST be encrypted and stored in a restricted-access administrative folder accessible solely by the CPFP to comply with GDPR.

Step 3: External referral, thresholds, and statutory cooperation

- **Referral thresholds:** External referral to Greek authorities is mandatory whenever there is reasonable suspicion, direct disclosure, or evidence of:
  - Immediate physical, sexual, or severe psychological risk to a child.
  - Suspected criminal offenses, abuse, or gross neglect under Greek child protection law.
- **No internal investigation:** Personnel must act on reasonable suspicion alone and are strictly prohibited from conducting independent inquiries or attempting to collect evidence prior to referring a case to authorities.
- **Competent national authorities:** When the referral threshold is met, the CPFP MUST report the case within 24 hours to the appropriate Greek child protection bodies:

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 14/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 14/23

    - **Judicial & Enforcement Authorities:** Prosecutor for Minors (*Εισαγγελέας Ανηλίκων*) or local Hellenic Police (*Ελληνική Αστυνομία*).
    - **Social Services & Emergency Helplines:** *National Child Protection Helpline - EKKA* (1107) or *The Smile of the Child* (*Το Χαμόγελο του Παιδιού* - 1056).
- **Cooperation with external investigations:** Simeio commits to fully cooperating with official police, prosecutorial, and social service inquiries. Staff members will share factual records (Annex D) upon formal request while complying with GDPR safeguards.
- **Funder notification:** If an incident involves project personnel or grant activities, the CPFP will inform the funding authority according to contractual obligations, ensuring participant privacy is maintained under GDPR.

7.4 Complaints, feedback, and whistleblowing mechanism

Simeio provides safe, accessible, and confidential channels for children, caregivers, staff, external contractors, and third parties to submit complaints, concerns, or feedback regarding child protection or general staff conduct.

Filing channels and designated contacts:

- **General complaints and concerns:** Reports can be submitted via email to contact@simeio.org.gr or handed directly to the CPFP.
- **Alternative conflict-of-interest channel:** If a complaint concerns the CPFP, the report should be submitted directly to Simeio's Director at antiphono@gmail.com.
- **Child-friendly complaint channels:** Minors participating in activities are informed of age-appropriate ways to express concerns, adapted to the activity format:
    - *In-person activities:* Direct verbal reporting to facilitators and/or a physical feedback box available on site.
    - *Online activities:* Direct messaging options or a dedicated contact email provided during session briefings.

Response process and mandatory timelines:

- **Acknowledgment:** All complaints will be acknowledged in writing (or verbally in an age-appropriate manner for minors) within 48 hours (2 working days).
- **Preliminary assessment:** The CPFP (or Director) conducts an initial review within 5 working days to evaluate non-emergency administrative complaints.
    - **Emergency Safety Override:** If a complaint received at any point indicates immediate risk, direct disclosure, or suspected abuse of a

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 15/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 15/23

minor, the 5-day assessment window is bypassed, and the 24-hour emergency escalation procedure in Section 7.3 applies immediately.

- **Formal resolution:** A full review and written response or action plan will be completed within 20 working days.

Protection against retaliation and good faith reporting:

- **Whistleblower protection:** Simeio strictly prohibits any form of retaliation, discrimination, or penalty against any child, parent, staff member, or third party who reports a concern or files a complaint in good faith. Identity confidentiality is strictly maintained throughout the process under GDPR.
- **Good faith reporting and misuse:** Protection against retaliation applies to all reports made in good faith (honest concerns, even if later proven unfounded). Submitting intentionally false or malicious accusations with the intent to harm individuals or the organization is considered a breach of conduct. If a minor or participant submits a knowingly false allegation, Simeio reserves the right to address the matter with their parent/guardian or restrict their participation in activities.

Simeio Legal Representatives

Ioanna Meitani
28/7/2026

Konstantinos Papaioannou
28/7/2026

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 16/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 16/23

ANNEX A

Code of Conduct Declaration Form

Child Safeguarding & Behavioral Agreement

I hereby acknowledge that I have received, read, and fully understood Simeio's Child Protection Policy (CPP), including Section 3: Code of Conduct and Behavioral Guidelines.

As a Tier 1 team member / associate working with or on behalf of Simeio, I agree to:

- Treat all minors with respect, dignity, and equity.
- Maintain open, visible, and well-supervised physical and digital environments during all project activities.
- Strictly adhere to boundary rules regarding physical contact, communication, and digital interactions.
- Respect media consent rules and never capture or publish images/videos of minors without explicit parental consent and the child's own agreement.
- Report any disclosure, suspicion, or potential breach of this policy through established channels within 24 hours.
- Comply with the zero-tolerance policy regarding any form of violence, abuse, harassment, or exploitation.

I understand that non-compliance with this Code of Conduct or any breach of Simeio's Child Protection Policy may lead to immediate suspension, termination of engagement, and potential legal or reporting actions to competent authorities.

Full Name: _____

Role / Position: _____

Project / Activity: _____

Date: ____ / ____ / 20__

Signature: _____

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 17/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 17/23

ANNEX B

Parental Consent and Child Assent Form Template

Simeio Youth Project Participation & Media Consent

1. General details

Project / Event name: _____

Date(s) of activity: ____ / ____ / 20__

Location / Platform: _____

Child's full name: _____

Child's date of birth / age: ____ / ____ / 20__ (Age: ____)

Parent / Guardian full name: _____

Contact email / phone: _____

2. Parental / Guardian consent *(Please check the boxes)*

[ ] **Participation:** I grant permission for my child to participate in the above-mentioned project/activity organized by Simeio.

[ ] **Data processing:** I consent to Simeio collecting and processing my child's basic personal data (e.g., name, age, workshop responses) solely for project implementation and reporting, in accordance with the Standard Privacy Notice (Annex C).

[ ] **Media & photo release:** I consent to Simeio capturing photographs, video, and audio recordings of my child during activities, to be used in project publications, website updates, and EU reporting. I understand that full names will never be published alongside images.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 18/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 18/23

3. Child assent *(To be completed with/by the child)*

(Facilitators/parents should explain the activity to the child in an age-appropriate way).

Child's Statement: I have been told about the project activities. I agree to participate and understand that I can stop taking part or ask not to be filmed/photographed at any time.

[ ] **Child agrees to participate**

[ ] **Child agrees to photos/videos (if applicable)**

4. Right to withdraw

You or your child have the right to withdraw consent at any time without giving a reason by emailing contact@simeio.org.gr. Upon withdrawal, data processing will cease immediately, and any unpublished media files will be permanently deleted.

Parent/Guardian signature: _____

Date: ____ / ____ / 20__

Child signature (if 12+ years old): _____

Date: ____ / ____ / 20__

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 19/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 19/23

ANNEX C

STANDARD PRIVACY NOTICE (GDPR) FOR MINORS' DATA

(To be provided to Parents/Guardians and older children prior to data collection, research, or media recording)

1. Who we are (data controller)

Simeio (simeio.org.gr) is the Data Controller responsible for protecting your child's personal data. We are fully committed to complying with the EU General Data Protection Regulation (GDPR) and Greek Data Protection Law (4624/2019).

2. What information we collect

Depending on the specific activity (e.g., research, workshop, event), we may collect:

- Basic identification (child's name, age, parent/guardian contact details).
- Research or feedback responses (which are separated from the child's real name using code numbers).
- Media (photographs, video, or audio recordings) — only if you give explicit separate consent for this.

3. Why we collect it and how it will be used

We collect this data solely for the purposes of:

- Safely organizing and delivering the activities of project _____.
- Conducting academic or social research related to the project goals.
- Fulfilling mandatory reporting requirements for our EU/institutional funders.

Legal basis: We process this data based strictly on your informed consent.

4. Who has access to the data?

Your child's data is strictly confidential:

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 20/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 20/23

- Only authorized, background-checked Simeio project staff have access.
- Research data is pseudonymized (real names are replaced with codes) before analysis.
- We never sell your data and we will never share your child's identifiable information with external commercial third parties. Public reports or publications will only use anonymous data or pseudonyms.

5. How long we keep the data

We only keep your child's personal data for as long as required by our project grant agreement (typically 3 to 5 years after the official close of the project to allow for EU audits). Once this period expires, all digital and physical records are permanently and securely destroyed.

6. Your rights (and your child's rights)

Under the GDPR, you and your child have the right to:

- Access the personal data we hold about your child.
- Request correction if any information is inaccurate.
- Withdraw consent and request erasure (deletion) at any time, without giving a reason and without any negative consequences.
- Refuse to be photographed or recorded, while still being allowed to participate in the activity.

7. How to contact us or make a complaint

To exercise any of these rights, or if you have any questions about how we handle data, please contact our Child Protection Focal Person (CPFP) at:

- **Email:** im@simeio.org.gr
- **Phone:** (+30)6974454561

If you feel your data rights have been violated, you also have the right to file a complaint with the Hellenic Data Protection Authority (ΑΠΔΠΧ) via www.dpa.gr.

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 21/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 21/23

ANNEX D

CHILD SAFEGUARDING INCIDENT REPORT FORM

(To be completed by the person observing or receiving a disclosure of a safeguarding concern, or by the CPFP. Store securely and confidentially.)

1. General information

Date and time of report: _____

Name of person completing form: _____

Role/position: _____

Contact details: _____

2. Incident / disclosure details

Date, time, and location of incident or disclosure: _____

Child's identifier / code to preserve anonymity under GDPR: _____

Factual description of the concern or disclosure:

(Record facts only: what was directly seen, heard, or disclosed. Use exact words spoken by the child where possible. Do not include personal opinions, assumptions, or judgments.)

_____

_____

_____

_____

_____

_____

_____

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 22/23

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 22/23

3. Immediate actions taken

Immediate safety measures implemented:

_____

_____

Internal notification:

CPFP notified on: _____

Method: _____

4. External referral (to be completed by CPFP)

Action required:

__ Internal record only

__ Escalated to Greek authorities

Authority contacted (if applicable):

__ Hellenic Police / Prosecutor for Minors

__ National Line for Child Protection (1107)

__ Smile of the Child (1056)

Date and time of external referral: _____

Reference number / officer contact: _____

5. Sign-off

Reporter signature: _____ Date: _____

CPFP signature: _____ Date: _____

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : 79vaF_2gRnReOXPjYquKGQ

Page: 23/23

Επιβεβαιώνεται το γνήσιο. Υπουργείο Ψηφιακής Διακυβέρνησης / Verified by the Ministry of Digital Governance, Hellenic Republic
20260728112248+03'00'

Signature:
ΙΩΑΝΝΑ ΑΝΝΑ ΜΕΪΤΑΝΗ / IOANNA-ANNA MEITANI
Father's name: ΧΡΗΣΤΟΣ ΑΝΔΡΕΑΣ / CHRISTOS-ANDREAS
TIN: 061088399
Date of signature: 28/07/2026 11:22:41

Digital Document Certification

You may validate this document by scanning the QR code or entering the Document ID at docs.gov.gr/validate

Document code : unzpFsZaNSjZRxtjKDl5AA

Page: 23/23

Επιβεβαιώνεται το γνήσιο. Υπουργείο Ψηφιακής Διακυβέρνησης / Verified by the Ministry of Digital Governance, Hellenic Republic
20260728121223+03'00'

Signature:
ΚΩΝΣΤΑΝΤΙΝΟΣ ΠΑΠΑΪΩΑΝΝΟΥ / KONSTANTINOS PAPAIOANNOU
Father's name: ΑΠΟΣΤΟΛΟΣ / APOSTOLOS
TIN: 044158845
Date of signature: 28/07/2026 12:12:13