PRIVACY POLICY

Effective Date: January 1, 2026
Last Updated: May 29, 2026

ABOUT THIS POLICY

Protect Us Kids Foundation ("PUK," "we," "us," or "our") is a U.S.-based nonprofit organization dedicated to protecting children and youth worldwide from cyber-related crimes. We operate the website http://www.protect-us-kids.org and provide global services primarily to youth in rural and under-resourced communities (collectively, the "Services").

This Privacy Policy explains our practices regarding the collection, use, disclosure, and protection of personal information, with special emphasis on protecting children and vulnerable populations we serve. This Policy is designed to comply with applicable U.S. federal and state laws, the General Data Protection Regulation (GDPR), and international child protection standards.

By using our Services, you acknowledge that you have read and understood this Privacy Policy and our Safeguarding & Child Protection Policy, which work together to ensure the safety and privacy of all individuals, especially children.

OUR COMMITMENT TO CHILD SAFETY

PUK's mission centers on protecting children. This Privacy Policy operates in conjunction with our Safeguarding & Child Protection Policy to ensure:

- Children's data is collected only when necessary and with appropriate consent
- Enhanced protections for personal information of individuals under 18
- Compliance with the UN Convention on the Rights of the Child (CRC), particularly Articles 2, 3, 12, 16, 19, and 34
- Alignment with the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography
- Adherence to the WeProtect Model National Response Strategy
- Zero tolerance for exploitation, abuse, or misuse of children's information

DEFINITIONS

"Service" means the http://www.protect-us-kids.org website and all related programs, platforms, and services operated by Protect Us Kids Foundation.

"Personal Data" means any information relating to an identified or identifiable natural person.

"Child" or **"Minor"** means any individual under the age of 18, as defined in Article 1 of the UN Convention on the Rights of the Child.

"Sensitive Personal Information" includes information about a child's identity, location, school, health, family circumstances, images, videos, or any data that could be used to identify, contact, or locate a child.

"Usage Data" means data collected automatically through use of the Service, such as IP addresses, browser type, pages visited, time spent on pages, and diagnostic data.

"Cookies" means small data files stored on your device that enable certain functionality and tracking.

"Data Controller" means the entity that determines the purposes and means of processing personal data. For this Privacy Policy, PUK is the Data Controller.

"Data Processor" means any entity that processes data on behalf of the Data Controller.

REGULATORY COMPLIANCE FRAMEWORK

UNITED STATES REGULATIONS:

This Privacy Policy is designed to comply with:

- Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA) where applicable
- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- California Online Privacy Protection Act (CalOPPA)
- Virginia Consumer Data Protection Act (VCDPA)
- Colorado Privacy Act (CPA)
- Connecticut Data Privacy Act (CTDPA)
- Utah Consumer Privacy Act (UCPA)
- State-specific data breach notification laws
- Nonprofit compliance requirements under IRS regulations

INTERNATIONAL REGULATIONS:

- General Data Protection Regulation (GDPR) - European Union
- UK GDPR and Data Protection Act 2018 - United Kingdom
- Personal Information Protection and Electronic Documents Act (PIPEDA) - Canada
- Australian Privacy Principles (APPs) - Australia
- Applicable data protection laws in countries where we provide services

CHILD PROTECTION STANDARDS:

- UN Convention on the Rights of the Child (CRC)
- Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography
- WeProtect Global Alliance standards
- National Center for Missing & Exploited Children (NCMEC) reporting requirements
- International Centre for Missing & Exploited Children (ICMEC) guidelines

INFORMATION WE COLLECT

1. INFORMATION COLLECTED FROM CHILDREN

We recognize that children have special privacy rights. When we collect information from or about children under 18, we:

- Obtain verifiable parental/guardian consent before collecting personal information from children under 13 (COPPA requirement)
- Limit collection to information reasonably necessary for participation in our programs
- Never condition a child's participation on disclosure of more information than necessary
- Maintain strict confidentiality and security measures
- Comply with all applicable child protection laws and regulations

Information we may collect from or about children includes:

- First name only (never full names without consent)
- Age or age range (not specific birthdate)
- General geographic location (city/region, never specific addresses)
- Program participation data
- Anonymous feedback and survey responses
- With appropriate consent: contact information for program communications

WE NEVER COLLECT FROM CHILDREN:

- Social Security numbers or national identification numbers
- Full home addresses or precise geolocation data
- School names or identifying information without explicit consent

- Financial information
- Biometric data
- Any unnecessary personal information

2. INFORMATION COLLECTED FROM ADULTS

When adults use our Services, we may collect:

Personal Identifiers:

- Full name
- Email address
- Phone number
- Mailing address
- Organization/affiliation (for professionals and partners)

Professional Information:

- Role or position
- Organization type
- Areas of expertise or interest
- Professional credentials (for verified child protection professionals)

Communication Data:

- Content of messages sent to us
- Support requests and correspondence
- Newsletter subscriptions and preferences

3. AUTOMATICALLY COLLECTED INFORMATION

Usage Data:

- IP address (anonymized where possible)
- Browser type and version
- Device type and operating system
- Pages visited and features accessed
- Time and date of visits
- Duration of visits
- Referring website addresses
- Click patterns and navigation paths

Technical Data:

- Device identifiers

- Log files
- Error reports and diagnostic data
- Performance metrics

Location Data:

- General geographic location (country, state/region, city)
- We do NOT collect precise GPS coordinates without explicit consent
- Location services can be disabled in device settings

4. COOKIES AND TRACKING TECHNOLOGIES

We use cookies and similar technologies for:

Strictly Necessary Cookies:

- Essential for website functionality
- Enable security features
- Remember login status

Preference Cookies:

- Remember your settings and choices
- Language preferences
- Accessibility settings

Analytics Cookies:

- Understand how visitors use our Services
- Measure and improve performance
- Identify technical issues

You can control cookies through your browser settings. Note that disabling certain cookies may limit functionality of our Services.

We do NOT use:

- Third-party advertising cookies
- Cross-site tracking cookies
- Social media tracking pixels (without consent)

5. INFORMATION FROM THIRD PARTIES

We may receive information from:

- Partner organizations (with appropriate agreements)

- Law enforcement or child protection agencies (for reporting purposes)
- Payment processors (limited to transaction confirmation)
- Professional references (for employment screening)

All third-party data sharing is governed by strict agreements ensuring child safety and privacy protection.

6. ARTIFICIAL INTELLIGENCE AND AUTOMATED PROCESSING

We may use AI-enabled tools and cloud services in the course of its operations. When AI tools or automated systems process personal data, the following protections apply:

- PUK does not use automated decision-making that produces legal or similarly significant effects on individuals — including decisions regarding program eligibility, service access, or safeguarding actions — without meaningful human oversight and intervention
- PUK does not use AI systems to profile children or create behavioral predictions about minors
- Where AI-powered tools are used in program delivery, data analysis, or communications, PUK ensures that personal data processed by those tools is subject to the same protections described in this Privacy Policy, including data minimization, purpose limitation, and security requirements
- PUK requires that AI-enabled cloud services and third-party processors handling PUK data do not use PUK data — including children's data — to train AI models unless PUK has provided explicit, documented authorization
- Individuals have the right to request information about whether their personal data has been processed by an AI system and to request human review of any AI-assisted decision that affects them

HOW WE USE INFORMATION

PROGRAM DELIVERY:

We use collected information only for legitimate purposes:

- Provide and maintain our Services
- Deliver online safety education and resources
- Facilitate participation in programs and events
- Communicate about program activities
- Provide technical support

CHILD PROTECTION:

- Identify and report child sexual abuse material (CSAM) to NCMEC
- Detect and prevent online exploitation
- Maintain safeguarding records as required by policy
- Collaborate with law enforcement when legally required
- Support investigations of child abuse

ORGANIZATIONAL OPERATIONS:

- Process donations and maintain donor records
- Communicate with supporters and stakeholders
- Send newsletters and program updates (opt-out available)
- Respond to inquiries and requests
- Comply with legal and regulatory obligations

RESEARCH AND IMPROVEMENT:

- Analyze Service usage to improve programs
- Conduct research on online child safety (anonymized data only)
- Develop safety solutions and technologies
- Measure program effectiveness
- Identify emerging threats and trends

LEGAL AND COMPLIANCE:

- Comply with applicable laws and regulations
- Respond to legal requests and court orders
- Protect rights, property, and safety of PUK, users, and the public
- Prevent fraud, abuse, and illegal activity
- Enforce our terms and policies

LEGAL BASIS FOR PROCESSING (GDPR)

For individuals in the European Economic Area (EEA), UK, or other GDPR-applicable jurisdictions, we process personal data based on:

- Consent: You have given clear consent for specific purposes
- Contract: Processing is necessary to fulfill our agreement with you
- Legal Obligation: Required to comply with the law (e.g., CSAM reporting)
- Vital Interests: Necessary to protect a child's life or safety
- Public Interest: Performing tasks in the public interest (child protection)

- Legitimate Interests: Necessary for our legitimate interests, provided these are not overridden by your rights

For children's data, we rely primarily on parental consent, legal obligations, vital interests, and public interest grounds.

DATA SHARING AND DISCLOSURE

1. SERVICE PROVIDERS

We do not sell, rent, or trade personal information. We share information only in limited circumstances:

We may share data with trusted third parties who:

- Assist with website hosting and maintenance
- Provide email and communication services
- Process donations and payments
- Perform data analysis (anonymized data only)
- Support technical operations

All service providers must:

- Sign strict data protection agreements
- Comply with our child protection standards
- Use data only for specified purposes
- Maintain appropriate security measures
- Undergo background checks if handling child data

2. PARTNER ORGANIZATIONS

We may share limited data with:

- Schools and educational institutions (with consent)
- Community organizations in service areas (with appropriate safeguards)
- Research partners (anonymized data only)
- Other child protection organizations (under strict agreements)

All partnerships require:

- Signed agreements affirming child protection principles
- Compliance with the more restrictive privacy policy
- Regular compliance monitoring
- Mutual commitment to safeguarding standards

3. LAW ENFORCEMENT AND CHILD PROTECTION AUTHORITIES

We are legally required to report to:

- National Center for Missing & Exploited Children (NCMEC): Any reports of child sexual abuse or exploitation received through any means, including suspected CSAM discovered during research
- Local Law Enforcement: When we have reasonable belief that a child is in immediate danger or has been subjected to abuse
- Child Protective Services: When required by law in applicable jurisdictions
- International Authorities: As required by local laws in countries where we operate

Reports are made in accordance with:

- 18 U.S.C. § 2258A (reporting requirements)
- State mandatory reporting laws
- Local laws in international jurisdictions
- Our Safeguarding & Child Protection Policy protocols

4. LEGAL REQUIREMENTS

We may disclose information when required to:

- Comply with court orders, subpoenas, or legal process
- Respond to lawful government requests
- Protect against legal liability
- Enforce our terms and policies
- Investigate potential violations
- Protect rights, property, and safety
- 5. BUSINESS TRANSFERS

In the event of a merger, acquisition, reorganization, or asset sale:

- Personal data may be transferred to the new entity
- We will provide notice before transfer
- The new entity must honor this Privacy Policy
- Enhanced protections apply to children's data
- We will seek appropriate consent where required

INTERNATIONAL DATA TRANSFERS

SAFEGUARDS FOR INTERNATIONAL TRANSFERS:

As a U.S.-based organization serving global communities, we may transfer data internationally.

- Standard Contractual Clauses (SCCs): We use EU-approved SCCs for transfers to countries

without adequacy decisions

- Adequacy Decisions: We rely on recognized adequacy determinations where applicable
- Binding Corporate Rules: Applied within our organizational structure
- Specific Consents: Obtained when required for transfers
- Enhanced Protections for Children: Additional safeguards for any international transfer of children's data

COUNTRY-SPECIFIC CONSIDERATIONS:

We assess data protection laws in each country where we operate and implement appropriate measures including:

- Local data residency requirements
- Regional privacy law compliance
- Cultural and contextual considerations
- Enhanced security for high-risk regions
- Your consent to this Privacy Policy, followed by submission of information, represents agreement to international transfer with these protections in place.

DATA RETENTION

GENERAL RETENTION PERIODS:

We retain personal data only as long as necessary for legitimate purposes:

- Program Participant Data: Duration of participation plus 2 years
- Donor Records: 7 years (IRS requirement for nonprofits)
- Employment Records: Duration of employment plus 7 years
- Safeguarding Records: Indefinitely for substantiated concerns; per policy for unsubstantiated reports
- Usage Data: 12-24 months unless required for security
- Cookie Data: Typically expires within 12 months
- Marketing Communications: Until you unsubscribe plus 30 days

CHILD-SPECIFIC RETENTION:

- Children's Personal Data: Minimum necessary period, typically not exceeding participation period plus 1 year
- Child Protection Reports: Maintained according to Safeguarding Policy and legal requirements
- Parental Consent Records: Duration of child's participation plus 3 years

EXCEPTIONS:

Data may be retained longer when:

- Required by law or regulation
- Necessary for ongoing legal proceedings
- Related to substantiated child protection concerns
- Essential for public interest purposes (child safety)

SECURE DELETION:

When retention periods expire, we:

- Securely delete or anonymize data
- Remove all identifying information
- Use industry-standard deletion methods
- Maintain deletion logs for accountability

DATA SECURITY

TECHNICAL SAFEGUARDS:

Protecting information, especially children's data, is our highest priority.

- Encryption: All data transmitted using TLS/SSL encryption (minimum TLS 1.2)
- Storage Security: Encrypted databases and secure servers
- Access Controls: Role-based access with principle of least privilege
- Authentication: Multi-factor authentication for staff accessing sensitive data
- Network Security: Firewalls, intrusion detection, and regular security monitoring
- Secure Development: Following OWASP guidelines and secure coding practices

CRYPTOGRAPHIC STANDARDS AND QUANTUM READINESS:

- PUK monitors the evolving post-quantum cryptographic threat landscape and its implications for long-term data protection
- PUK requires its cloud service providers and data processors to maintain encryption standards aligned with current best practices
- Providers shall demonstrate migration planning toward post-quantum cryptographic standards published by the National Institute of Standards and Technology (NIST)
- This is particularly important for data categories with long retention periods — including safeguarding records and donor records — which may be vulnerable to harvest-now-decrypt-later attack scenarios
- PUK's encryption posture is reviewed annually as part of its security policy review cycl

ORGANIZATIONAL SAFEGUARDS:

- Background Checks: Criminal background checks for all staff with potential child contact
- Training: Mandatory privacy and child protection training for all personnel
- Policies: Comprehensive safeguarding and information security policies
- Incident Response: Documented procedures for data breaches and security incidents
- Regular Audits: Periodic security assessments and compliance reviews
- Vendor Management: Due diligence and monitoring of third-party processors

PHYSICAL SAFEGUARDS:

- Secure Facilities: Access-controlled office spaces
- Device Security: Encrypted laptops and mobile devices
- Clean Desk Policy: Secure storage of physical documents
- Visitor Controls: Escort requirements and sign-in procedures

CHILD-SPECIFIC PROTECTIONS:

- Anonymization: Children's identifying information removed when possible
- Segregated Storage: Children's data maintained separately with enhanced security
- Limited Access: Only authorized personnel with legitimate need and proper clearance
- No Public Disclosure: Children's information never published without explicit consent
- Image Protection: Photographs and videos stored securely with consent documentation

BREACH NOTIFICATION:

In the event of a data breach:

- We will investigate and assess the scope and impact
- Notify affected individuals without undue delay (within 72 hours when feasible)
- Report to relevant authorities as required by law
- Take immediate steps to mitigate harm
- Implement corrective measures to prevent recurrence
- Provide support resources to affected individuals

While we implement robust security measures, no system is 100% secure. We cannot guarantee absolute security but commit to using commercially reasonable and industry-leading practices.

YOUR PRIVACY RIGHTS

RIGHTS UNDER GDPR (EEA/UK RESIDENTS):

We respect your rights and provide mechanisms to exercise them.

- Right to Access: Request confirmation of what personal data we hold and obtain a copy
- Right to Rectification: Request correction of inaccurate or incomplete data
- Right to Erasure ("Right to be Forgotten"): Request deletion of your data in certain circumstances
- Right to Restriction: Request limitation of processing in specific situations
- Right to Data Portability: Receive your data in a structured, commonly used format
- Right to Object: Object to processing based on legitimate interests or for direct marketing
- Right to Withdraw Consent: Withdraw consent at any time where we rely on consent
- Right to Lodge a Complaint: File a complaint with your supervisory authority

RIGHTS UNDER U.S. STATE LAWS (CCPA/CPRA and similar):

- Right to Know: Request information about data collection, use, and sharing
- Right to Delete: Request deletion of personal information
- Right to Correct: Request correction of inaccurate information
- Right to Opt-Out: Opt-out of "sales" or "sharing" of personal information (Note: We do not sell or share data for advertising)
- Right to Limit: Limit use of sensitive personal information
- Right to Non-Discrimination: Exercise rights without discriminatory treatment

CHILDREN'S PRIVACY RIGHTS:

- Parental Access: Parents/guardians can review their child's information
- Parental Control: Parents/guardians can request deletion of child's data
- Consent Withdrawal: Parents/guardians can withdraw consent at any time
- Participation Withdrawal: Right to discontinue program participation
- No Retaliation: Children and families face no negative consequences for exercising rights

HOW TO EXERCISE YOUR RIGHTS:
Contact us at:

- Email: info@protect-us-kids.org
- Phone: 866.772.3354 or 866.7.SAFEKID
- Mail: Privacy Officer, Protect Us Kids Foundation, 1629 K St NW, Suite 300, Washington, DC 20006
- Website: https://www.protect-us-kids.org/privacy-policy/

We will:

- Verify your identity before responding (to protect your information)
- Respond within legally required timeframes (typically 30-45 days)
- Provide clear explanation if we cannot fulfill your request
- Not charge a fee unless requests are excessive or unfounded

For children's data requests, we require verification of parental/guardian authority.

CHILDREN'S PRIVACY PROTECTIONS

COPPA COMPLIANCE (CHILDREN UNDER 13):

Before collecting personal information from children under 13, we:

1. Provide notice to parents/guardians including:

- Types of information collected
- How information will be used
- Whether information will be disclosed to third parties
- Parental rights regarding the information

2. Obtain verifiable parental consent through:

- Consent forms with signature verification
- Video conference confirmation
- Government-issued ID verification
- Other FTC-approved methods

3. Allow parents/guardians to:

- Review their child's information
- Direct us to delete their child's information
- Refuse further collection or use of information

4. Maintain reasonable security for children's information

TEEN PRIVACY (AGES 13-17):
For teens, we:

- Encourage parental involvement while respecting developing autonomy
- Seek parental consent for sensitive programs or data collection
- Provide clear privacy information teens can understand
- Offer direct communication channels for privacy concerns
- Limit data collection to program necessities

AI AND CHILDREN'S DATA:

PUK applies enhanced protections when AI systems interact with or process children's data:

- AI-powered services that interact directly with children (including chatbots, recommendation engines, or automated communications) shall not be deployed on PUK platforms without a documented child data protection impact assessment and explicit approval
- Children's personal data shall not be used as input for AI model training, fine-tuning, or improvement by any PUK vendor or service provider
- AI-generated content directed at children shall be reviewed by qualified personnel for age-appropriateness, accuracy, and alignment with PUK's safeguarding standards before deployment
- PUK does not subject children to automated decision-making without human oversight
- Parents and guardians have the right to request information about any AI processing of their child's data and to object to such processing

SPECIAL PROTECTIONS FOR VULNERABLE CHILDREN:
For children in under-resourced communities and high-risk situations:

- Enhanced confidentiality measures
- Additional review of consent processes
- Cultural and linguistic accommodations
- Trauma-informed approaches to data collection
- Coordination with local child protection services

ONLINE SAFETY AND CHILD PROTECTION

DETECTING AND REPORTING CSAM:

- Staff Training: All personnel trained to recognize and report CSAM
- Immediate Reporting: Any suspected CSAM reported immediately to NCMEC CyberTipline
- No Investigation: Staff do not open suspected CSAM materials
- Support Availability: Management provides support to staff encountering CSAM
- International Reporting: Overseas personnel report to local authorities per applicable law

PROTECTING CHILDREN IN OUR PROGRAMS:

- No One-on-One Contact: Adults avoid being alone with any child
- Group Interactions: All child contact is observable and interruptible

- Monitored Communications: Use of school/work email platforms for any necessary communication
- No Personal Contact: Staff prohibited from seeking personal information about children outside programs
- Image Consent: Written parental consent required before photographing children
- Anonymous Case Sharing: Case information anonymized when used for training or research

TRIGGER WARNINGS AND SAFE SPACES:

When presenting child protection content:

- Content warnings at the start of presentations
- Acknowledgment of likely survivor presence
- Permission to step away without explanation
- Resources for support
- Anonymized case examples only

CONFIDENTIALITY AND INFORMATION HANDLING

CASE INFORMATION:

• Anonymization: All case details anonymized before sharing
• Explicit Permission: Permission obtained before using case details in training
• Identifying Information Changed: Names, locations, and other identifiers modified
• Secure Communication: Case information shared only through secure channels
• Prompt Deletion: Email correspondence with case information deleted when support concludes

RESEARCH AND ANALYSIS:

- Aggregate Data: Research uses anonymized, aggregated data
- No Reidentification: Measures to prevent reidentification of individuals
- Ethical Review: Research protocols reviewed for privacy and child protection
- Minimal Data: Only minimum necessary data used for research purposes

PRESENTATIONS AND PUBLICATIONS:

- No CSAM: Presentations never contain child sexual abuse material
- Obscured Images: Images used in professional contexts are obscured or stock photos
- Consent Required: Any non-stock images require documented consent
- No Child Identification: Children never identifiable in public materials
- No Location Information: Addresses, school names, and precise locations excluded

THIRD-PARTY SERVICES

PAYMENT PROCESSORS:

Protect Us Kids Foundation processes donations through trusted third-party financial service providers. These providers securely handle payment information on our behalf and are responsible for protecting donor financial data.

Our current payment processing channels may include:

PayPal Giving Fund / PayPal Charity
Online donations processed through PayPal are handled by PayPal, Inc., a third-party payment processor. Protect Us Kids Foundation does not store full credit card or bank account information submitted through PayPal.

Banking Institutions (ACH / Direct Deposit)
Electronic transfers and direct deposits are processed through regulated financial institutions and banking networks. These transactions are protected under applicable banking security standards.

Check Donations
Checks are processed through our financial institution using standard banking deposit procedures. Physical records are handled securely and retained only as required for accounting and compliance purposes.

Current payment processors:

- PayPal Giving Fund: https://www.paypal.com/webapps/mpp/ua/privacy-full
- Stripe: https://stripe.com/privacy
- Apple Store In-App Payments: https://www.apple.com/legal/privacy/
- Google Play In-App Payments: https://www.google.com/policies/privacy/

CLOUD SERVICE PROVIDERS:

- Website Hosting: Secure, GDPR-compliant hosting providers
- Email Services: Encrypted email platforms
- Data Storage: Encrypted cloud storage with U.S. or EU data centers
- All providers sign Data Processing Agreements (DPAs)

ANALYTICS:

- Google Analytics: Used with IP anonymization and data minimization
- Privacy-focused alternatives considered

- No tracking of children without appropriate consent
- Users can opt out using browser extensions or settings

DO NOT TRACK SIGNALS

Currently, there is no industry standard for Do Not Track (DNT) signals.

Our approach:

- We do not respond to DNT signals from browsers
- We provide opt-out mechanisms for cookies and tracking
- We limit tracking technologies to essential and functional purposes
- We do not engage in cross-site behavioral advertising
- Our tracking is primarily for security, functionality, and service improvement

Users can control tracking through:

- Browser cookie settings
- Opting out of analytics cookies
- Using privacy-focused browsers or extensions
- Adjusting privacy settings in their accounts

LINKS TO THIRD-PARTY SITES

Our Services may contain links to external websites and services.

Important notes:

- We are not responsible for third-party privacy practices
- We recommend reviewing privacy policies of linked sites
- Links do not imply endorsement or control
- Third-party sites may have different privacy standards
- Exercise caution when providing information to third parties

We specifically review linked resources to ensure they:

- Maintain appropriate child safety standards
- Do not contain harmful or inappropriate content
- Align with our mission and values

MARKETING AND COMMUNICATIONS

NEWSLETTERS AND UPDATES:

We send communications about:

- Program updates and opportunities
- Online safety resources and education
- Fundraising appeals and impact reports
- Policy changes and organizational news

You can:

- Opt out at any time using the unsubscribe link
- Update communication preferences in your account
- Choose specific types of communications to receive
- Contact us to be removed from all marketing lists

We will not:

- Send unsolicited commercial emails to children
- Share your contact information with third parties for marketing
- Send excessive communications
- Continue sending after you opt out (except transactional emails)

TRANSACTIONAL COMMUNICATIONS:
We may send necessary communications about:

- Program enrollment confirmation
- Account security notices
- Legal and policy updates
- Responses to your inquiries
- Service-related announcements

These cannot be opted out of while using our Services.

DATA PROTECTION OFFICER

We have designated a Privacy Officer responsible for:

- Overseeing privacy compliance
- Handling privacy inquiries and requests
- Coordinating with data protection authorities
- Monitoring data protection practices
- Investigating privacy concerns

- Training staff on privacy requirements

Contact our Privacy Officer:

- Email: info@protect-us-kids.org
- Mail: Privacy Officer, Protect Us Kids Foundation, 1629 K St NW, Suite 300, Washington, DC 20006

SUPERVISORY AUTHORITIES

EEA/UK RESIDENTS:

You have the right to lodge a complaint with a supervisory authority in your country of residence, place of work, or place of alleged infringement.

EU Data Protection Authorities: https://edpb.europa.eu/about-edpb/board/members_en

UK Information Commissioner's Office: https://ico.org.uk/

U.S. RESIDENTS:

Federal Trade Commission: https://www.ftc.gov/

State Attorneys General offices handle consumer privacy complaints.

POLICY UPDATES AND CHANGES

NOTIFICATION OF CHANGES:

We may update this Privacy Policy periodically to reflect:

- Changes in our practices
- New legal requirements
- Service enhancements
- Feedback and best practices

We will:

- Update the "Effective Date" at the top of this Policy
- Provide notice of material changes via:
    - Email to registered users
    - Prominent notice on our website
    - In-app notifications where applicable
- Seek new consent if required by law
- Provide reasonable notice before changes take effect (typically 30 days)

MATERIAL CHANGES:
Changes we consider material include:

- New data collection practices
- Expanded data sharing or disclosure
- Reduced privacy protections
- Changes to children's data handling
- Modified retention periods
- New third-party processors

Your continued use of our Services after changes take effect constitutes acceptance of the updated Policy. If you disagree with changes, discontinue use and contact us about data deletion.

REVIEWING UPDATES:
We encourage you to:

- Review this Policy periodically
- Check the effective date
- Read update notices carefully
- Contact us with questions
- Exercise your rights if you disagree with changes

SPECIAL COMPLIANCE PROVISIONS

NONPROFIT COMPLIANCE:

As a tax-exempt organization under IRC Section 501(c)(3):

- We maintain donor privacy and confidentiality
- Donor information is not sold, traded, or rented
- Donors may remain anonymous
- We comply with IRS reporting and recordkeeping requirements
- Financial information is handled securely

STATE CHARITABLE SOLICITATION REQUIREMENTS:

We comply with state registration and disclosure requirements for charitable solicitations.

GRANT AND FUNDING COMPLIANCE:

When required by funders:

- We maintain specific data retention periods

- Provide anonymized program data for evaluation
- Comply with funder privacy and security requirements
- Report outcomes using de-identified information

ACCESSIBILITY

We are committed to making this Privacy Policy accessible to all individuals.

Available formats:

- Web-based version (current)
- Large print available upon request
- Plain language summary available
- Audio version available upon request
- Translations available in languages of communities we serve

To request alternative formats:

Contact us at info@protect-us-kids.org or call 866.772.3354

QUESTIONS AND CONTACT INFORMATION

GENERAL INQUIRIES:

For any privacy-related questions, concerns, or requests:

Email: info@protect-us-kids.org

Phone: 866.772.3354

Website: https://www.protect-us-kids.org

PRIVACY-SPECIFIC MATTERS:

Email: info@protect-us-kids.org

Privacy Officer: Protect Us Kids Foundation

Mail: 1629 K St NW, Suite 300, Washington, DC 20006

CHILD PROTECTION CONCERNS:

To report child sexual abuse or exploitation:

UNITED STATES

NCMEC CyberTipline: https://www.cybertipline.org or 1-800-843-5678

FBI: https://www.fbi.gov/how-we-can-help-you/parents-and-caregivers-protecting-your-kids

Know2Protect Tipline (U.S. Department of Homeland Security): https://www.dhs.gov/know2protect/how-to-report

INTERNATIONAL

INHOPE: https://www.inhope.org/ - Global network of reporting hotlines; users select their country to report suspected child sexual abuse material.

For general child safety concerns:

Email: info@protect-us-kids.org

EUROPEAN REPRESENTATIVE (GDPR):

Email: info@protect-us-kids.org

RESPONSE TIMEFRAME:

We strive to respond to all inquiries within:

- 5 business days: Initial acknowledgment
- 30 days: Complete response to privacy rights requests
- 45 days: Extended response for complex requests (with notification)

RELATED POLICIES

This Privacy Policy should be read in conjunction with:

- Child Safeguarding & Child Protection Policy
- Terms of Service
- Cookie Policy
- Data Retention Policy
- Information Security Policy
- Acceptable Use Policy

All policies are available at: https://www.protect-us-kids.org/policies/

GOVERNING LAW

This Privacy Policy is governed by:

- U.S. federal laws applicable to nonprofits

- District of Columbia law (our principal place of business)
- Applicable international data protection laws
- Local laws in jurisdictions where we operate

Disputes are subject to resolution in accordance with our Terms of Service.

EFFECTIVE DATE AND VERSION

Current Version: 2.0

Effective Date: January 1, 2026

Previous Version Date: December 31, 2023

Document History:

- Version 1.0 (July 28, 2018): Initial privacy policy
- Version 1.5 (December 31, 2023)
- Version 2.0 (Decemnber 31, 2025): Comprehensive update for enhanced child protection, regulatory compliance, and international operations

This policy was last reviewed: December 31, 2025

Next scheduled review: December 31, 2027

© 2026 Protect Us Kids Foundation. All rights reserved.

This Privacy Policy represents our commitment to protecting the privacy and safety of all individuals, especially children and vulnerable populations. We continuously evaluate and improve our practices to maintain the highest standards of care and compliance.

For the most current version of this Privacy Policy, visit:

https://www.protect-us-kids.org