Data Retention Policy

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

1. PURPOSE AND SCOPE

This Data Retention Policy establishes guidelines for how long Protect Us Kids Foundation ("PUK") retains different types of data and information.

PURPOSE:

- Comply with legal and regulatory requirements
- Support our mission and operational needs
- Protect individual privacy rights
- Maintain data security and minimize risk
- Preserve important organizational records

SCOPE:

This policy applies to all data collected, created, or maintained by PUK, including:

- Program participant information
- Donor and supporter records
- Employee and volunteer information
- Organizational and financial documents
- Communications and correspondence
- Website and digital platform data
- Safeguarding and child protection records

2. GUIDING PRINCIPLES

- Retention Minimization: Keep data only as long as necessary for legitimate purposes
- Child Protection Priority: Enhanced protections and limited retention for children's data
- Legal Compliance: Meet all applicable legal and regulatory requirements
- Secure Disposal: Properly destroy data when retention periods expire
- Documented Process: Maintain clear records of retention decisions and destruction
- Regular Review: Periodically assess and update retention schedules

3. RETENTION SCHEDULES

PROGRAM PARTICIPANT DATA

Children Under 18:

- Active Participation: Duration of participation
- Post-Participation: 1 year after participation ends
- Parental Consent Records: Duration of participation + 3 years
- Exception: Anonymized program data may be retained indefinitely for research

Adults:

- Active Participation: Duration of participation
- Post-Participation: 2 years after participation ends
- Marketing Communications: Until unsubscribe + 30 days

DONOR AND FINANCIAL RECORDS

Donor Information:

- Donation Records: 7 years (IRS requirement for 501(c)(3) organizations)
- Grant Records: 7 years after grant period ends
- Financial Statements: 7 years
- Tax Returns and Supporting Documents: Permanent
- Annual Reports: Permanent
- Audit Records: 7 years

Payment Processing:

- We do not store credit card information (handled by processors)
- Transaction confirmations: 7 years

EMPLOYMENT AND VOLUNTEER RECORDS

Personnel Files:

- Background Checks: Duration of service + 7 years

Volunteer Applications:

- Onboarded Candidates: Move to volunteer file
- Not Onboarded: 2 years (for potential EEOC claims)

SAFEGUARDING AND CHILD PROTECTION RECORDS

Incident Reports:

- Substantiated Concerns: Indefinite retention
- Unsubstantiated Concerns: Per policy guidelines and legal requirements
- Reports to NCMEC/Authorities: Indefinite retention of confirmation

Training Records:

- Staff Training Documentation: Duration of volunteership + 7 years
- Policy Acknowledgment Forms: Duration of employment/service + 3 years

COMMUNICATIONS AND CORRESPONDENCE

Email and Messages:

- General Business Email: 3 years
- Policy-Related Communications: 7 years
- Legal or Regulatory Correspondence: 7 years or duration of matter
- Donor Communications: 7 years
- Case-Related Communications: Per safeguarding retention schedule
- Routine/Administrative: 1 year

Social Media:

- Published Content: Indefinite (public record)
- Direct Messages: 2 years
- Engagement Analytics: 2 years

CONTRACTS AND LEGAL DOCUMENTS

- Active Contracts: Duration of contract + 7 years
- Expired Contracts: 7 years after expiration
- Partnership Agreements: Duration + 7 years
- Insurance Policies: Permanent
- Intellectual Property Documents: Permanent
- Litigation Files: Duration of matter + 7 years

WEBSITE AND DIGITAL DATA

- Website Analytics: 24 months
- Server Logs: 12 months (security) or 90 days (routine)
- User Account Data: Duration of account + 1 year

- Cookie Data: Per Cookie Policy (typically 12-26 months)
- Technical Support Tickets: 3 years
- Security Incident Records: 7 years

AI GOVERNANCE AND CRYPTOGRAPHIC RECORDS

AI Application Inventory:

- Current version maintained continuously
- Superseded versions retained for 3 years

AI Vendor Assessment Records:

- Duration of vendor relationship + 7 years

AI Incident Records:

- 7 years (consistent with security incident records)
- AI Tool Usage Logs and Audit Records:
- 3 years

AI Output Disclosure Records:

- 3 years

Shadow AI Detection and Remediation Records:

- 3 years

Algorithmic Fairness Testing Records (if applicable):

- Duration of AI system use + 7 years

Cryptographic Inventory Records:

- Current version maintained continuously
- Superseded versions retained for 7 years

Post-Quantum Readiness Assessment Records:

- 7 years

Cloud Provider Cryptographic Assurance Documentation:

- Duration of provider relationship + 7 years

ORGANIZATIONAL RECORDS

- Board Meeting Minutes: Permanent
- Articles of Incorporation/Bylaws: Permanent
- Annual Reports to Board: Permanent
- Strategic Plans: Permanent
- Policies and Procedures: Current version + superseded versions for 7 years
- Media Coverage/Press Releases: Permanent (archival)

4. EXCEPTIONS TO RETENTION SCHEDULES

Data may be retained beyond standard periods when:

LEGAL HOLDS:

- Litigation, investigations, or audits are pending or reasonably anticipated
- Government requests or subpoenas require retention
- Legal counsel advises extended retention

CHILD PROTECTION:

- Substantiated safeguarding concerns require indefinite retention
- Ongoing investigations necessitate extended retention
- Legal or regulatory authorities request continued retention

HISTORICAL VALUE:

- Records have significant historical or archival value to the organization
- Records document important milestones or achievements

ACTIVE USE:

- Records continue to serve a legitimate business purpose
- Ongoing programs or relationships require access to historical data

5. DATA DESTRUCTION PROCEDURES

When retention periods expire, data must be securely destroyed unless an exception applies.

SECURE DESTRUCTION METHODS:

Electronic Data:

- Secure deletion using DoD 5220.22-M standard (7-pass) or equivalent
- Cryptographic erasure (destroying encryption keys)
- Physical destruction of storage media (shredding, degaussing)
- Certified data destruction services for sensitive information
- Verification that AI-enabled cloud services have completed deletion of PUK data in accordance with PUK's retention schedules, including confirmation that data has not been retained for AI model training purposes

Physical Records:

- Cross-cut shredding (minimum 5/32" x 1-1/2" particles)
- Pulping or incineration for high-security documents
- Witnessed destruction for highly sensitive records
- Certificate of destruction obtained from vendors

DESTRUCTION REQUIREMENTS:

- Document what was destroyed, when, by whom, and method used
- Maintain destruction logs for audit purposes (7 years)
- Use authorized personnel or certified vendors only
- Verify destruction before removing from inventory
- For data processed by AI-enabled cloud services, obtain written confirmation from the provider that data has been purged from all systems, including training pipelines, caches, and derivative datasets

6. ANONYMIZATION AND DE-IDENTIFICATION

As an alternative to destruction, data may be anonymized for continued use:

- Remove all direct identifiers (names, contact information, ID numbers)
- Remove indirect identifiers that could lead to re-identification
- Aggregate data to prevent individual identification
- Apply appropriate anonymization techniques
- Verify anonymization effectiveness
- Document anonymization process

Anonymized data may be retained indefinitely for:

- Research and analysis
- Program evaluation
- Statistical reporting
- Service improvement

7. ROLES AND RESPONSIBILITIES

CHIEF EXECUTIVE OFFICER / PRIVACY OFFICER:

- Overall responsibility for policy implementation
- Approve retention schedule updates
- Ensure compliance with legal requirements
- Oversee data protection program

DEPARTMENT HEADS / PROGRAM MANAGERS:

- Implement retention schedules for their areas
- Train staff on retention requirements
- Coordinate data destruction
- Identify records for legal holds

ALL STAFF AND VOLUNTEERS:

- Follow retention schedules
- Do not destroy data prematurely
- Report potential legal holds
- Handle data securely throughout its lifecycle

IT STAFF:

- Implement technical retention controls
- Execute secure data destruction
- Maintain backup and archival systems
- Monitor compliance with retention policies

8. COMPLIANCE AND MONITORING

ANNUAL REVIEW:

- Review retention schedules annually
- Update based on legal changes
- Assess compliance with policy
- Identify areas for improvement

AUDITS:

- Periodic compliance audits
- Review destruction logs
- Verify proper implementation
- Document findings and remediation

TRAINING:

- Include retention policy in staff onboarding
- Provide annual refresher training

- Communicate policy updates promptly
- Document training completion

9. LEGAL AND REGULATORY CONSIDERATIONS

This policy is designed to comply with:

- IRS requirements for 501(c)(3) organizations (7-year retention)
- Department of Labor requirements (payroll, benefits)
- EEOC requirements (employment records)
- GDPR (data minimization, storage limitation)
- State data breach notification laws
- Federal and state child protection laws
- Grant and contract requirements
- Industry best practices

Legal counsel should be consulted for:

- Litigation holds
- Subpoenas or legal requests
- Uncertainty about retention requirements
- Policy interpretation questions

10. POLICY UPDATES

This policy will be reviewed and updated:

- Annually at minimum
- When legal or regulatory requirements change
- When organizational needs change
- Based on audit findings or incidents

Updates require approval by:

- Chief Executive Officer
- Board of Directors (for major changes)

11. RELATED POLICIES

This policy should be read in conjunction with:

- Privacy Policy
- Safeguarding & Child Protection Policy
- Information Security Policy
- Document Management Policy
- Records Management Policy

12. CONTACT INFORMATION

Questions about this policy should be directed to:

Privacy Officer

Protect Us Kids Foundation

Email: info@protect-us-kids.org

Phone: 866.772.3354

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

© 2026 Protect Us Kids Foundation. All rights reserved.