Acceptable Use Policy

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

1. PURPOSE AND SCOPE

This Acceptable Use Policy ("AUP") defines appropriate use of Protect Us Kids Foundation's ("PUK") technology resources, systems, and information assets.

PURPOSE:

- Protect PUK's information, systems, and reputation
- Ensure compliance with legal and ethical standards
- Protect children and vulnerable populations we serve
- Maintain a safe and productive work environment
- Prevent misuse, abuse, or illegal activity

SCOPE:

This policy applies to:

- All employees, interns, volunteers, contractors, board members, and temporary staff
- All organizational technology resources (computers, phones, tablets, networks, accounts)
- Personal devices used for organizational work
- All uses of technology resources whether on-site or remote

Technology resources include but are not limited to:

- Computers, laptops, tablets, smartphones
- Network infrastructure and internet access
- Email and communication systems
- Software and applications
- Cloud services and online platforms
- Data storage and file sharing systems
- Printers, copiers, and other peripherals

2. GENERAL PRINCIPLES

- Primary Use: Technology resources are provided for organizational purposes. Limited personal use is permitted within reason.
- Professional Conduct: Users must conduct themselves professionally and ethically in all technology use.
- Child Safety First: All use must align with our mission to protect children and must not put children at risk.
- Legal Compliance: Users must comply with all applicable laws and regulations.
- No Expectation of Privacy: PUK reserves the right to monitor and review use of organizational systems. Users should have no expectation of privacy.
- Responsible Use: Users are responsible for their actions and must exercise good judgment.
- Resource Conservation: Use resources efficiently and avoid waste.

3. ACCEPTABLE USES

Technology resources may be used for:

ORGANIZATIONAL PURPOSES:

- Job-related duties and responsibilities
- Professional development and training
- Authorized organizational communications
- Program delivery and participant services
- Research and education related to our mission
- Collaboration with partners and stakeholders

LIMITED PERSONAL USE:

- Brief personal communications (email, phone calls)
- Accessing personal accounts during breaks
- Emergency personal matters

Personal use is acceptable when it:

- Does not interfere with work duties
- Does not consume excessive resources
- Does not violate any provision of this policy
- Does not involve prohibited activities (see Section 4)

4. PROHIBITED USES

The following uses are strictly prohibited:

CHILD SAFETY VIOLATIONS:

- Accessing, creating, storing, transmitting, or distributing child sexual abuse material (CSAM)
- Grooming, exploiting, or endangering children in any way
- Using technology to contact children inappropriately
- Sharing children's personal information without authorization
- Violating our Safeguarding & Child Protection Policy

ILLEGAL ACTIVITIES:

- Violating any federal, state, or local laws
- Intellectual property infringement (piracy, unauthorized copying)
- Hacking, unauthorized access, or security breaches
- Fraud, identity theft, or financial crimes
- Harassment, stalking, or threats
- Distributing illegal content

HARMFUL OR OFFENSIVE CONTENT:

- Accessing, creating, or distributing pornography or sexually explicit material
- Hate speech, discriminatory content, or extremist material
- Violence, weapons, or dangerous activities
- Profanity or offensive language in professional communications
- Gambling or gaming (except educational purposes)

MISUSE OF RESOURCES:

- Excessive personal use interfering with work
- Streaming video/audio for personal entertainment
- Large personal file storage
- Cryptocurrency mining
- Running personal businesses
- Downloading or installing unauthorized software

SECURITY VIOLATIONS:

- Sharing passwords or account credentials
- Attempting to bypass security controls
- Introducing malware, viruses, or harmful code
- Unauthorized access to systems or data

- Tampering with security software or logs
- Social engineering or phishing attempts

COMMUNICATIONS VIOLATIONS:

- Representing personal views as organizational positions
- Unauthorized use of PUK name, logo, or branding
- Sending spam or mass unsolicited emails
- Participating in chain letters or pyramid schemes
- Harassing, threatening, or abusive communications
- Disclosing confidential or proprietary information

NETWORK VIOLATIONS:

- Excessive bandwidth consumption
- Intentionally degrading network performance
- Unauthorized network scanning or sniffing
- Creating or connecting to unauthorized networks
- Bypassing content filters or proxies

5. EMAIL AND COMMUNICATION GUIDELINES

PROFESSIONAL EMAIL USE:

- Use professional language and tone
- Include clear subject lines
- Use organizational email for work purposes
- Include signature with contact information
- Respond to work emails in a timely manner

EMAIL SECURITY:

- Do not open suspicious attachments or click unknown links
- Verify sender before responding to sensitive requests
- Report phishing attempts
- Use encryption for sensitive information
- Do not send passwords via email

EMAIL CONTENT:

- Do not send confidential information to personal accounts
- Be mindful that emails can be forwarded and archived
- Avoid sending when emotional; review before sending

- Use "Reply All" judiciously
- Keep distribution lists current

INSTANT MESSAGING:

- Use approved platforms only
- Maintain professional conduct
- Do not share sensitive information via IM
- Set status appropriately
- Log out when away from device

6. INTERNET AND WEB USE

ACCEPTABLE INTERNET USE:

Work-related research and information gathering

- Professional development and online learning
- Communication with partners and stakeholders
- Accessing approved cloud services
- Brief personal browsing during breaks

WEB BROWSING GUIDELINES:

- Exercise caution when downloading files
- Verify website authenticity before providing information
- Be aware that browsing activity may be monitored
- Report inappropriate content or security concerns
- Use HTTPS sites when providing sensitive information

PROHIBITED WEB ACTIVITIES:

- Accessing inappropriate, illegal, or offensive websites
- Streaming personal entertainment during work hours
- Online shopping (except for organizational purposes)
- Personal social media during work time (excessive)
- Downloading illegal or pirated content

7. SOCIAL MEDIA GUIDELINES

PROFESSIONAL SOCIAL MEDIA:

- Use separate accounts for personal and organizational purposes

- Follow organization's social media policies
- Clearly identify when speaking personally vs. on behalf of PUK
- Protect confidential and proprietary information
- Maintain professional image

PERSONAL SOCIAL MEDIA:

- Do not claim to represent PUK without authorization
- Do not share confidential information
- Do not disparage PUK, staff, or stakeholders
- Be aware that online activity may reflect on PUK
- Respect privacy of children, donors, and participants

CHILD PROTECTION:

- Never share identifying information about children we serve
- Do not "friend" or connect with program participants on personal accounts
- Obtain proper consent before posting photos of children
- Report concerning content to appropriate authorities
- Follow our Safeguarding & Child Protection Policy

8. SOFTWARE AND APPLICATIONS

SOFTWARE USAGE:

Use only licensed and approved software

- Do not install software without authorization
- Keep software updated with security patches
- Report software issues to IT support
- Do not use organizational licenses for persona

PROHIBITED SOFTWARE:

- Pirated or illegally obtained software
- Peer-to-peer file sharing applications
- Hacking tools or password crackers
- Software that poses security risks
- Personal VPNs or proxy services (without approval)

CLOUD SERVICES:

- Use only approved cloud services
- Do not store organizational data on personal cloud accounts
- Configure security settings appropriately
- Understand data location and retention policies
- Use organizational accounts for organizational work

8. SOFTWARE AND APPLICATIONS

AI TOOL AUTHORIZATION:

- Artificial intelligence tools — including generative AI platforms (such as ChatGPT, Gemini, Claude, Copilot, and similar services), AI-powered writing assistants, AI image generators, and AI-enabled cloud features — are subject to PUK's technology approval process
- Only AI tools that have been reviewed and approved may be used for organizational purposes
- Approval status of specific AI tools shall be maintained in PUK's AI application inventory
- Questions about whether a specific tool qualifies as an AI tool should be directed to IT or a supervisor

PROHIBITED AI USES:

- Entering children's personally identifiable information, safeguarding records, case details, or any Restricted data into any AI platform — including approved tools unless that tool has been specifically authorized for Restricted data
- Entering donor financial information, personnel records, background check results, or other Confidential data into external AI platforms
- Using AI tools to generate content that impersonates PUK, its staff, partners, or program participants
- Using AI to create synthetic media (deepfakes), fabricated images of children, or any content that could be used for exploitation, grooming, or harassment
- Using AI tools to circumvent PUK security controls, generate malicious code, or bypass content filters
- Using personal AI accounts for organizational work without approval
- Using AI tools to conduct unauthorized research, surveillance, or data collection about individuals — especially children

ACCEPTABLE AI USES:

With appropriate approval and in compliance with this policy, AI tools may be used for:

- Drafting and editing general communications, reports, and educational content (subject to human review before publication)
- Research and information gathering on topics related to PUK's mission
- Professional development and learning
- Administrative tasks that do not involve Restricted or Confidential data

AI CONTENT DISCLOSURE:

- When AI tools are used to substantially generate content for external communications, program materials, grant applications, policy documents, or public-facing publications, personnel shall disclose AI involvement to their supervisor
- All AI-generated content must be reviewed for accuracy, bias, and alignment with PUK's mission and values before use
- Personnel remain responsible for the accuracy and appropriateness of any content they submit, regardless of whether AI tools were used in its creation

PERSONAL USE OF AI:

- Limited personal use of AI tools during breaks is subject to the same restrictions as other personal technology use under Section 3 of this policy
- Personal AI use must not involve PUK data, systems, or accounts
- Personal AI use must not violate any provision of the Prohibited AI Uses section above

MONITORING:

- PUK reserves the right to monitor the use of AI tools on organizational systems and networks in accordance with Section 12 of this policy
- AI tool usage may be audited to ensure compliance with this policy and PUK's information classification requirements

9. MOBILE DEVICES

ORGANIZATIONAL DEVICES:

- Primarily for work purposes
- Keep devices secure with passcodes
- Report lost or stolen devices immediately
- Do not jailbreak or root devices
- Install only approved applications

PERSONAL DEVICES (BYOD):

- Must meet security requirements
- Separate work data when possible
- Accept remote wipe capability
- Keep personal content separate from work content
- Follow same usage policies as organizational devices

MOBILE SECURITY:

- Enable device encryption
- Use screen lock (passcode or biometric)
- Keep operating system updated
- Install security updates promptly
- Be cautious on public Wi-Fi

10. DATA HANDLING AND PRIVACY

DATA PROTECTION:

- Handle data according to classification (see Information Security Policy)
- Store sensitive data securely
- Use encryption for restricted data
- Limit data collection to what is necessary
- Follow data retention schedules

PRIVACY REQUIREMENTS:

- Respect privacy rights of all individuals
- Enhanced protections for children's data
- Obtain appropriate consents
- Share information only with authorized parties
- Follow Privacy Policy requirements

DATA DISPOSAL:

- Securely delete data when no longer needed
- Shred physical documents
- Wipe devices before disposal or reassignment
- Do not discard media in regular trash
- Follow Data Retention Policy

11. REMOTE WORK AND TELEWORK

REMOTE WORK REQUIREMENTS:

- Use VPN for accessing organizational systems
- Ensure home network is secured
- Maintain confidentiality in home environment
- Keep work area private during video calls
- Follow same policies as in-office work

HOME OFFICE SECURITY:

- Lock screens when away from device
- Secure documents and devices
- Prevent family/roommates from accessing work devices
- Use headphones for confidential calls
- Shred confidential documents

PUBLIC SPACES:

- Avoid accessing restricted data in public
- Use privacy screens
- Be aware of surroundings
- Use VPN on public Wi-Fi
- Do not leave devices unattended

12. MONITORING AND PRIVACY

PUK reserves the right to monitor:

- Email and other electronic communications
- Internet browsing and web activity
- Network traffic and bandwidth usage
- System and application logs

- File access and transfers
- Device location and usage

PURPOSES OF MONITORING:

Ensure policy compliance

- Maintain security
- Prevent misuse
- Investigate incidents
- Optimize resources
- Legal compliance

PRIVACY EXPECTATIONS:

- Users have no expectation of privacy when using organizational resources
- Personal use may also be monitored
- Monitoring is conducted in accordance with applicable laws
- Results may be used for disciplinary action

13. REPORTING VIOLATIONS

REPORTING REQUIREMENTS:

- Report suspected policy violations to supervisor or IT
- Report security incidents immediately
- Report child safety concerns to designated personnel
- Report illegal activity to appropriate authorities

REPORTING METHODS:

- Direct communication with supervisor
- Email to IT or Privacy Officer
- Confidential hotline (if available)
- Anonymous reporting accepted

NO RETALIATION:

- No retaliation for good-faith reporting
- Reports handled confidentially
- Investigation conducted fairly
- Protections for whistleblowers

14. CONSEQUENCES OF VIOLATIONS

Violations of this policy may result in:

- Verbal or written warning
- Mandatory retraining
- Loss of access privileges
- Suspension (with or without pay)
- Termination of employment or volunteer status
- Legal action (civil or criminal)
- Reporting to law enforcement

FACTORS IN DETERMINING CONSEQUENCES:

- Severity of violation
- Intent (accidental vs. deliberate)
- Impact on organization or individuals
- Prior violations
- Whether violation involves children or illegal activity

15. SPECIAL CONSIDERATIONS

REASONABLE ACCOMMODATIONS:

- Accommodations provided for disabilities
- Assistive technology use approved
- Modified policies when needed for accessibility

UNION OR EMPLOYMENT AGREEMENTS:

- This policy does not supersede collective bargaining agreements
- Conflicts resolved in favor of employment agreements

VOLUNTEERS AND INTERNS:

- Same policies apply
- Limited access based on role
- Supervision appropriate to position

16. ACKNOWLEDGMENT AND AGREEMENT

All users must:

- Read and understand this policy
- Sign acknowledgment form
- Complete required training
- Ask questions if uncertain
- Review policy updates

By using PUK technology resources, users acknowledge:

- They have read and understand this policy
- They agree to comply with all provisions
- They understand consequences of violations
- They have no expectation of privacy
- They will report violations

17. POLICY UPDATES

This policy may be updated:

- To address new technologies
- In response to incidents
- To meet legal requirements
- Based on organizational needs

Users will be notified of material changes.

Continued use constitutes acceptance of updates.

18. RELATED POLICIES

Read in conjunction with:

- Cybersecurity & Information Security Policy
- Privacy Policy
- Data Retention Policy
- Safeguarding & Child Protection Policy

- Social Media Policy
- Remote Work Policy

19. QUESTIONS AND ASSISTANCE

For questions about this policy:

IT Support: [IT email/phone]
Supervisor: [Contact your direct supervisor]

HR/Administration: [HR email/phone]

For security concerns: IT Support

For child safety concerns: safeguarding@protect-us-kids.org

For privacy questions: privacy@protect-us-kids.org

20. APPROVAL

This policy has been approved by:

Executive Director: _____ Date: _____

Board Chair: _____ Date: _____
