

**CHILDREN INTERNET PROTECTION ACT (CIPA) POLICY
INTERNET SAFETY, ACCEPTABLE USE, ONLINE PROTECTION &
TECHNOLOGY PROTECTION POLICY**

I. PURPOSE

Head Start of Rockland, Inc. (HSOR) is committed to providing a safe, secure, and educational technology environment for children, families, staff, volunteers, consultants, contractors, and authorized users. This policy establishes requirements governing the use of HSOR's computers, networks, internet access, electronic communications systems, and technology resources.

This policy complies with the Children's Internet Protection Act (CIPA), applicable federal and state laws, Head Start Program Performance Standards (HSPPS), confidentiality requirements, and HSOR's Code of Ethics.

All individuals granted access to HSOR technology resources are responsible for ensuring that such resources are used appropriately, ethically, securely, and solely for authorized purposes.

Questions regarding this policy should be directed to the Executive Director, Human Resources Director, or Information Technology Administrator (VirtuIT).

II. POLICY STATEMENT

Access to the Internet through HSOR's network is a privilege, not a right, and carries responsibilities reflecting responsible and ethical use.

Internet access must be approved by the employee's supervisor and granted based upon a legitimate business, educational, or programmatic need.

By accessing the Internet through HSOR systems, users acknowledge and agree to comply with this policy and all other applicable HSOR policies and procedures.

Violations of this policy may result in revocation of system privileges, disciplinary action up to and including termination of employment, contract termination, legal action, and/or referral to law enforcement authorities.

III. DEFINITIONS

A. Minor(s)

For purposes of this policy, a minor is any individual under the age of seventeen (17).

B. Technology Resources.

Technology resources include but are not limited to:

- Computers
- Laptops
- Tablets
- Mobile devices
- Servers
- Internet access
- Wireless networks
- Electronic mail systems
- Cloud-based applications
- Software programs
- Digital communication platforms

C. Technology Protection Measure

A technology protection measure is a software application, cloud-based filtering service, firewall solution, or other technology designed to block or filter internet content.

D. Harmful to Minors

"Harmful to minors" shall have the meaning established under the Children's Internet Protection Act (CIPA) and applicable federal law.

IV. INTERNET SAFETY POLICY

A. Access by Minors to Inappropriate Matter

HSOR shall utilize filtering and monitoring systems designed to prevent minors from accessing:

- Obscene content;
- Child pornography;
- Material harmful to minors;
- Violent or graphic content;
- Gambling websites;
- Hate speech or extremist content;
- Other content deemed inappropriate by HSOR.

All children using technology must be supervised by authorized staff.

B. Safety and Security of Minors

HSOR shall take reasonable measures to ensure the safety and security of minors while using technology.

Children will not access:

- Social networking websites;
- Chat rooms;
- Instant messaging platforms;
- Electronic communication systems; unless specifically approved, educationally appropriate, and directly supervised by staff.

C. Unauthorized Access and Online Activities

Users are prohibited from:

- Hacking or attempting to gain unauthorized access;
- Circumventing security systems or internet filters;
- Accessing restricted accounts;
- Introducing malware, ransomware, viruses, or harmful code;
- Altering system configurations without authorization;
- Using another individual's username or password.

Any suspected security incident must be reported immediately to your immediate supervisor and to VirtulT Helpdesk line at noc@virtuitsystems.com

D. Protection of Personal Information

Users shall not disclose confidential information concerning children, families, staff, volunteers, or HSOR operations through the internet or electronic communications.

Prohibited disclosures include:

- | | |
|----------------------|---|
| • Addresses | • Financial information |
| • Telephone numbers | • Personnel information |
| • Birth dates | • Personally identifiable information (PII) |
| • Health information | |
| • Child records | |
| • Family information | |

All users must comply with HSOR confidentiality policies and applicable privacy laws (see confidentiality Policy).

E. Restricting Access to Harmful Materials

HSOR shall implement technology protection measures that restrict access to content considered harmful to minors. Determinations regarding inappropriate content will be made by HSOR administration and the Board of Directors consistent with CIPA requirements.

F. Digital Citizenship and Online Behavior Education

Consistent with CIPA requirements, HSOR shall educate minors, when developmentally appropriate, regarding:

- Appropriate online behavior;
- Internet safety;
- Cyberbullying awareness and prevention;
- Responsible digital citizenship;
- Safe online interactions; and
- Protection of personal information.

Staff shall model and reinforce responsible technology use.

V. TECHNOLOGY PROTECTION MEASURES

A. Technology Protection Measures

HSOR shall implement and maintain technology protection measures on all computers, mobile devices, networks, and internet-enabled systems owned, leased, operated, or managed by the agency.

HSOR utilizes enterprise-level technology protection systems, including:

- Firewalls;
- Content filtering software;
- Anti-malware solutions; and
- Network monitoring tools.

These systems are designed to block or filter access to:

- Obscene material;
- Child pornography;
- Harmful material;
- Violent or graphic content;
- Gambling-related content;
- Hate speech or extremist content;
- Malware and phishing websites; and
- Other content determined inappropriate for children.



B. Filtering and Monitoring

Technology protection measures shall provide:

- Content filtering and website blocking;
- User activity monitoring;
- Website access logs;
- Blocked website reports;
- Security alerts and notifications; and
- Audit trails documenting filter operation and system activity.

All Internet activity conducted through HSOR technology resources may be monitored, logged, and reviewed.

C. Network Security Safeguards

HSOR shall maintain:

- Firewall protection;
- Antivirus and anti-malware software;
- Secure wireless network access;
- Password-protected systems;
- Multi-factor authentication where appropriate; and
- Regular software updates and security patch management.

D. Authorized Disabling of Technology Protection Measures

Only the Executive Director, Information Technology Administrator (VirtuIT), or designee may temporarily disable or modify a technology protection measure for an adult user when necessary for:

- Bona fide research;
- Professional development;
- Educational purposes; or
- Other lawful business activities.

Requests must be documented and approved prior to implementation.

Technology protection measures shall never be disabled for minors.

E. Technology Protection Responsibilities

Executive Director Responsibilities

- Ensure compliance with CIPA;
- Approve filtering and monitoring procedures; and
- Ensure annual policy review.

Information Technology Administrator Responsibilities

- Install, maintain, and update filtering systems;
- Monitor cybersecurity risks;
- Maintain documentation demonstrating filter operation;
- Produce reports upon request; and
- Address security incidents and vulnerabilities.

Staff Responsibilities

- Supervise children using technology;
- Report filter failures and security concerns immediately; and
- Refrain from bypassing or disabling security measures.

VI. ACCEPTABLE USE OF TECHNOLOGY

A. Authentication and Account Security

All users must access HSOR systems through assigned credentials.

Each user is responsible for maintaining the confidentiality of:

- Usernames
- Passwords
- Security tokens
- Authentication devices

Sharing passwords or permitting unauthorized individuals to use assigned credentials is strictly prohibited.

Users are responsible for all activity conducted under their assigned credentials. Although users may be assigned usernames and passwords, they should not expect communications transmitted through HSOR systems to be private or confidential from organizational review.



B. MONITORING OF TECHNOLOGY USE

HSOR reserves the right to monitor, inspect, review, access, and audit all technology resources at any time and without prior notice.

Monitoring may include:

- Internet activity
- Email communications
- Network access logs
- Downloads and uploads
- Cloud storage activity
- Electronic files
- Device usage

Monitoring is conducted to:

- Ensure compliance with policies;
- Protect organizational assets;
- Investigate misconduct;
- Maintain cybersecurity;
- Ensure the safety of children and families.

Use of HSOR technology constitutes consent to such monitoring.

C. ACCEPTABLE PERSONAL USE

Limited personal use of the internet may be permitted provided that:

- It occurs during non-working time;
- It does not interfere with job duties;
- It does not consume excessive network resources;
- It complies with all HSOR policies.

All HSOR technology resources remain primarily for business and program purposes.

D. SOCIAL MEDIA AND PUBLIC COMMUNICATIONS

When using public forums, social media, blogs, discussion groups, or other online platforms in a personal capacity, users shall clearly indicate that their opinions are their own and do not represent HSOR.

Users shall not:

- Represent themselves as speaking on behalf of HSOR without authorization;
- Post confidential information;
- Post photographs or videos of children without appropriate written parental consent;
- Post photographs of staff without authorization;
- Make statements that could damage HSOR's reputation.

E. ETHICAL USE OF THE INTERNET

Users shall comply with all federal, state, and local laws and conduct themselves professionally and ethically when using technology resources.

The following activities are prohibited:

- Accessing pornography;
- Viewing child sexual abuse material;
- Gambling;
- Harassment;
- Discrimination;
- Hate speech;
- Racism;
- Threatening communications;
- Cyberbullying;
- Fraud;
- Illegal activity;
- Offensive or obscene communications.

Electronic communications must reflect professional standards and align with HSOR's Code of Ethics.

F. ELECTRONIC COMMUNICATIONS

Users will exercise the same care when creating electronic communications as they would when preparing official written correspondence.

Users should assume that electronic communications may be:

- Archived;
- Retrieved;
- Audited;
- Reviewed during investigations;
- Subject to legal disclosure requirements.

All users must comply with HSOR's Electronic Mail Policy and Confidentiality Policy.

G. DOWNLOADING SOFTWARE AND FILES

To protect HSOR's systems and data:

Users may not:

- Download software without prior written approval;
- Install unauthorized applications;
- Download games;
- Download executable programs;
- Alter device configurations.

All downloaded files must be scanned using approved security software before use. Users must comply with all copyright, trademark, licensing, and intellectual property laws. Any suspected malware infection, virus, or system compromise must be reported immediately. Users may not install unauthorized internet service providers or online access services on HSOR-owned devices.

H. DIGITAL CITIZENSHIP AND ONLINE BEHAVIOR EDUCATION

Consistent with CIPA requirements, HSOR shall educate minors, when developmentally appropriate, regarding:

- Appropriate online behavior;
- Internet safety;
- Cyberbullying awareness and prevention;
- Responsible digital citizenship;
- Safe online interactions;
- Protection of personal information.

Staff shall model and reinforce responsible technology use.

STAFF RESPONSIBILITIES

Staff members shall:

- Supervise children's technology use;
- Enforce this policy;
- Report inappropriate online activity;
- Participate in cybersecurity and internet safety training;
- Protect confidential information;
- Maintain professional standards while using technology resources.

VII. PUBLIC NOTICE AND BOARD REVIEW REQUIREMENTS

Prior to adoption of this policy, HSOR shall provide public notice and conduct a public meeting of the Board of Directors to review and approve the policy as required by CIPA.

Documentation shall include:

- Public notice;
- Meeting agenda;
- Meeting minutes; and
- Board approval records.

Policy Council shall also review and approve this policy in accordance with Head Start governance requirements.



VIII. RECORD RETENTION

HSOR shall maintain documentation demonstrating compliance with CIPA for a minimum of ten (10) years, including:

- Internet Safety Policy;
- Technology Protection Measure documentation;
- Board and Policy Council approval records;
- Public notices and meeting minutes;
- Descriptions of filtering technologies utilized;
- Filter activity reports and logs;
- Evidence demonstrating operation of filtering systems;
- FCC Forms 479 and 486, when applicable; and
- Corrective action documentation related to CIPA compliance.

IX. VIOLATIONS

Violations of this policy may result in:

- Suspension of Internet privileges;
- Revocation of network access;
- Corrective action;
- Disciplinary action up to and including termination;
- Civil liability; and
- Criminal prosecution where appropriate.

X. POLICY REVIEW

This policy shall be reviewed annually and revised as necessary to maintain compliance with CIPA, Head Start requirements, cybersecurity best practices, and applicable federal and state laws.

XI. POLICY APPROVAL

Approved By: HSOR Board of Directors and Policy Council

Effective Date: May 23, 2026

Supersedes: Previous Internet Use Policy