STANDARD OPERATING PROCEDURE FOR INTERNET SERVICE PROVIDERS TO ENSURE CHILD ONLINE SAFETY

NATIONALE POSTCODE LOTERIJ

SCROL
Safety for Children and their Rights OnLine

Terre des Hommes Netherlands

ISPAN

CWIN

NYESHR
Estd:-2012

STANDARD OPERATING PROCEDURE FOR INTERNET SERVICE PROVIDERS TO ENSURE CHILD ONLINE SAFETY

Prepared by:
Suvash Khadka

Reviewed by:
Kapil Aryal
Aavash Khadka
Ram Krishna Pariyar
Santosh Maharjan

Layout and design:
Binod Shivabhakti

Published by:
Internet Service Providers Association Nepal (ISPAN)
Center for Legal Research and Resource Development (CeLRRd)

Supported by:
Terre des Hommes Netherlands (TdH NL)

Published Year:
2024

PREFACE

Children Online Safety has been key initiatives of Internet Service Providers Association of Nepal (ISPAN), Center for Legal Research and Resource Development (CeLRRd) and Terre des Hommes Netherlands (TdH NL). After a series of events organized by both the organizations Supported by TdH NL under Safety of Children and their Rights online, the necessity for Standard Operating Procedure (SOP) for ISP to ensure Children Online Safety was felt

This Standard Operating Procedure (SOP) for Internet Service Providers (ISPs) outlines the necessary steps to protect children from online threats, child sexually abusive materials, while using internet services. It aims to create a safe and secure online environment for children by establishing clear procedures and guidelines. This SOP defines responsibilities, implements protective measures, and ensures compliance with legal and regulatory requirements. It also focuses on educating users, raising awareness, fostering collaboration, and promotes reporting of suspicious activities to the law enforcement agencies.

This SOP was reviewed and revised on June 27, 2024, at the 'Consultative Workshop on SOP for Internet Service Providers' held at Bogini Nagarkot Resort, Nagarkot. The workshop sought feedback from stakeholders, including ISPs, government agencies, law enforcement, and child protection organizations, to enhance online child safety measures.

TABLE OF CONTENTS

1. PURPOSE

The purpose of this Standard Operating Procedure (SOP) is to outline the procedures and guidelines for protecting children from online threats, sexually abusive materials, and crimes while using our internet services. This document serves as a comprehensive framework to ensure that our internet services provide a safe and secure online environment for children, safeguarding their well-being and protecting them from harmful content and activities.

By establishing clear procedures and guidelines, this SOP aims to:

- **Define Responsibilities:**

  Clearly delineate the roles and responsibilities of various stakeholders, including ISP management, customer service teams, technical teams, legal teams, and law enforcement agencies in ensuring child safety online.

- **Implement Protective Measures:**

  To stop children from accessing unsuitable content, prevent them from online grooming, bullying, harassment, and other harms, and reduce hazards, put in place efficient safeguards, including parental controls, and incident response protocols.

- **Compliance with Legal and Regulatory Requirements:**

  Make sure all applicable laws and rules—such as the Act Relating to Children (2018), the Electronic Transaction Act (2006), Crime Victim Protection Act (2018),) Directives to Regulate the Use of Social Media (2023) —that regulate child protection, privacy, and online safety are followed. Likewise, bylaws and directives issued by the regulator Nepal Telecommunications Authority Cyber Security Bylaw (2020), Internet Service Regulation Bylaw (2020), Online Child Protection Directives (2019).

- **Educate Users and Raise Awareness:**

  Develop educational resources, training programs, and awareness campaigns to educate users about online safety best practices, empower parents and guardians to monitor and manage their children's online activities, and raise awareness about the risks of online threats.

- **Foster Collaboration and Reporting:**

  Establish mechanisms for collaboration with law enforcement agencies, child protection organizations, and other stakeholders to address online threats and incidents effectively. Implement reporting mechanisms to enable users to report suspicious activities or content and facilitate timely responses.

- **Ensure Documentation and Continuous Improvement:**

  Maintain comprehensive documentation of all procedures, guidelines, and incidents related to child safety online. Conduct regular reviews, audits, and updates to enhance safety measures and adapt to evolving threats and technologies.

- **Complaint Handling:**

  Establish a clear and accessible complaint-handling mechanism for users to report online child abuse incidents, also to report to authorities.

2. RESPONSIBILITIES

In order to safeguard children from various threats prevalent online ISP should ensure the following roles and responsibilities:

2.1. ISP Management:

ISP should ensure that the following criteria are managed:

2.1.1. Strategic Planning and Implementation:

- Develop and enforce a comprehensive strategy for children's online safety.
- Allocate resources and budget for implementing safety measures and training programs.

2.1.2. Policy Development:

- Create and update policies related to children's online safety, privacy, and data protection.
- Ensure that all policies comply with local and international laws and regulations.

2.1.3. Oversight and Accountability:

- Monitor the effectiveness of safety measures and ensure accountability across all teams.
- Conduct regular reviews and audits of safety protocols and

practices.

2.1.4. Collaboration and Coordination:

- Coordinate efforts between different teams (Customer Service, Technical, Legal) to ensure seamless implementation of safety measures.
- Establish partnerships with external organizations, such as schools, NGOs, and law enforcement, to enhance online safety initiatives.

2.1.5. Communication and Transparency:

- Maintain open communication channels with customers regarding safety measures and updates.
- Ensure transparency in policies and procedures, providing clear guidelines on how customers can protect their children online.

2.2. Customer Service Team:

ISP should make a proper customer service team who perform the following operations:

2.2.1. Customer Support and Guidance:

- Provide 24/7 assistance to customers on setting up and managing parental controls and online safety features.
- Offer guidance on best practices for online safety, including how to recognize and report suspicious activities.

2.2.2. Educational Resources:

- Create and disseminate instructional resources, such as FAQs, tutorials, and brochures, on internet safety.

- Educate parents and children about digital hazards and safe online behaviour by holding workshops and webinars.

2.2.3. Feedback and Improvement:

- Get consumer opinions on safety features and how well they work.
- Work with the technical and management teams to implement improvements based on customer feedback.

2.2.4. Incident Reporting and Resolution:

- Assist customers in reporting incidents related to children's online safety.
- Ensure timely resolution of issues, coordinating with the Technical and Legal teams as necessary.

2.3. Technical Team:

ISP should develop a separate technical team with following responsibilities:

2.3.1. Implementation of Safety Technologies:

- Design, develop, and implement content filtering systems to block inappropriate content for Child Sexual Abuse Materials (as directed on Internet Service Regulation Bylaw (2020), Online Child Protection Directives (2019)).
- Deploy parental control tools and ensure they are user-friendly and effective.

2.3.2. System Maintenance and Updates:

- Regularly update filtering systems and safety tools to address new

threats and vulnerabilities.

- Monitor the performance of safety technologies and make necessary adjustments to enhance protection.

2.3.3. Security and Network Protection:

- Implement network-level security measures such as firewalls, anti-malware, and intrusion detection systems.
- Ensure the robustness of these measures through regular testing and updates.

2.3.4. Technical Support:

- Provide technical support to the Customer Service team for resolving complex issues related to safety features.
- Develop and maintain a knowledge base for common technical issues and their solutions.

2.4. Legal Team:

- A legal team should be established which cooperates with law enforcement agencies. This team should also be responsible for:

2.4.1. Compliance and Risk Management:

- Make sure that all online safety precautions abide by all applicable federal, provincial, and local-level laws, and international laws and regulations pertaining to data privacy and children protection.
- Assess risks on a regular basis to find possible legal problems and make sure mitigation plans are in place.

2.4.2. Policy and Contract Review:

- Draft and review policies, terms of service, and user agreements to ensure they reflect current legal standards and best practices for child safety.
- Ensure that contracts with third-party vendors include clauses that mandate compliance with child safety standards.

2.4.3. Training and Awareness:

- Provide training to all ISP employees on relevant laws and regulations concerning child safety online including technical training.
- Stay updated on legal developments and ensure the ISP's policies and practices are adjusted accordingly.

2.4.4. Incident Handling and Legal Response:

- Lead the legal response to incidents involving children's safety, working with law enforcement as required.
- Ensure that all legal protocols are followed during incident investigations and that customer data is protected.

3. PROCEDURES

The following are the procedures that ISP should follow.

3.1. Content Filtering:

ISP should implement and maintain content filtering systems to block access to websites containing explicit or Child Sexual Abuse Materials(as directed on Internet Service Regulation Bylaw (2020), Online Child Protection Directives (2019)) . The following are the approaches it should follow to ensure child safety:

3.1.1. Keyword Blocking:

Blocking websites or content based on pre-defined lists of keywords associated with harmful content (e.g., violence, child sexual abuse materials).

3.1.2. URL Blocking:

Blocking access to specific websites known to host harmful content. This relies on maintaining an up-to-date blacklist.

3.1.3. Category-Based Filtering:

Filtering websites based on pre-determined categories (e.g., gambling) which parents can then adjust according to their preferences.

3.1.4. Content Analysis Tools:

Utilizing automated systems that analyze text, images, and videos to identify potential harmful content. It is crucial that ISP regularly update and review the effectiveness of content filtering measures.

3.2. Parental Controls:

ISP should provide customers with access to parental control tools to manage and restrict their children's online activities. It needs to ensure:

3.2.1. Time Management:

ISP can allow parents to set time limits on internet usage to prevent excessive screen time. They should have features for:

- Setting daily or weekly time limits for internet usage.
- Scheduling access, allowing internet use only during certain hours as per customers demand (e.g., homework time, weekends).
- Instant pause or resume of internet access.

3.2.2. Usage Monitoring:

ISP should provide features for monitoring and tracking the child's internet activity to keep parents informed about their online behavior. The feature should include facilities for parents to:

- View browsing history, including visited websites and time spent on each site.
- Alerts for attempts to access blocked content or websites.
- Reports on internet usage patterns and trends.

3.2.3. Safe Search:

ISP should provide features to enable safe search settings on search engines to filter out inappropriate content (CSAM) from search results. The feature should include facilities for parents to:

- Automatically enforce safe search on popular search engines like Google, Bing, and YouTube.
- Lock safe search settings to prevent children from changing them.
- Collaborate with content providers, vendors, platforms as per necessity.

3.2.4. Application and Device Controls:

ISPs should provide features for controlling access to specific applications and devices connected to the home network. The feature should ensure parents privileges to:

- Block or limit access to certain apps, such as gaming, and chat applications which promote CSAM.
- Manage internet access for individual devices, ensuring that only authorized devices can connect to the network.

3.2.5. Remote Management:

ISP should allow parents to manage and control parental settings remotely. The feature should allow parents to:

- Track Web-based or mobile app interfaces used by their children for remote management of parental controls.
- Track real-time updates and changes to settings.

3.3. Education and Awareness:

To ensure online child safety, ISPs can implement various education and awareness programs tailored to different audiences, including parents, children, and educators. These programs should aim to increase understanding of online risks and equip users with the knowledge and tools to protect themselves and their families. Here are some effective education and awareness programs that ISPs can implement:

3.3.1. Online Safety Workshops and Webinars:

ISP should conduct programs such as regular workshops and webinars focused on online safety. The program should include:

- Sessions for parents on using parental controls and recognizing online threats.

- Workshops for children on safe internet practices, cyberbullying, and privacy.
- Collaboration with educational institutions to integrate workshops into the curriculum.

3.3.2. Educational Campaigns:

ISP should launch broad educational campaigns to raise awareness about online safety. The education campaigns should include:

- Social media campaigns using infographics, videos, and interactive content.
- Email newsletters with tips, updates, and resources on online safety.

3.3.3. Online Safety Portals:

ISP should develop an online safety portal on their website. The portal should have features such as:

- Comprehensive resources, including articles, videos, and FAQs on online safety.
- Interactive tools and quizzes to test knowledge and awareness.
- Links to external resources and helplines for additional support.

3.3.4. Parental Control Tutorials:

ISP should provide detailed tutorials on setting up and using parental controls. These tutorials should include:

- Step-by-step guides, both in written form and video tutorials.
- Live demonstrations and Q&A sessions.
- One-on-one support sessions for parents needing personalized assistance.

3.3.5. Collaboration with Schools and Educators:

ISP should partner with educational institutions to promote online safety. They should:

- Offer training for teachers on integrating online safety into their curriculum.
- Organize school events and activities focused on digital literacy and safety.

3.3.6. Cyberbullying Prevention Programs:

ISP should develop programs specifically aimed at preventing and addressing cyberbullying. It should include:

- Workshops and seminars for parents and children on recognizing and responding to cyberbullying.
- Support groups and counseling services for victims of cyberbullying.
- Resources for teachers on handling cyberbullying incidents in the classroom.

3.4. Reporting Mechanisms:

To ensure child safety online, ISPs should implement robust and user-friendly reporting mechanisms. Here are the key reporting mechanisms that ISPs should implement:

3.4.1. Easy-to-Access Reporting Tools:

ISP's should provide straightforward and easily accessible tools for reporting issues. These tools should ensure:

- Clearly visible report buttons on the ISP's website, customer portals, and mobile apps.
- Integration of report buttons within parental control software and content filtering tools.

- Quick access to reporting tools from any device connected to the ISP's network.

3.4.2. Multiple Reporting Channels:

ISP's should offer various channels through which users can report their concerns. The reporting channel should contain:

- Online forms that users can fill out to report issues.
- Email addresses dedicated to receiving reports of online threats or inappropriate content.
- Telephone hotlines for immediate reporting and assistance.
- In-app reporting features within ISP-provided applications.

3.4.3. Anonymous Reporting Options:

ISP's should allow users to report incidents anonymously to protect their identity. There should be mechanism for:

- Anonymous online forms and email submissions.
- Confidential handling of all reported information.
- Assurance that personal details will not be shared without consent.

3.4.4. Reporting Templates and Guides:

ISP's should provide standardized templates and guides to help users report issues effectively. The templates should include:

- Pre-filled templates for common issues such as cyberbullying, inappropriate content, and suspicious activities.
- Step-by-step guides on how to report different types of incidents.

3.4.5. Feedback and Follow-Up Mechanisms:

ISP's should ensure users receive feedback and updates on the status of their reports. These mechanism should include:

- Automatic confirmation emails upon receipt of a report.
- Regular updates on the progress of investigations and actions taken.
- Direct contact from the ISP's support team for follow-up and resolution.

3.4.6. Integration with Law Enforcement and Regulatory Bodies:

ISP's should coordinate with law enforcement and regulatory bodies for serious incidents. There should be provisions for:

- Direct reporting channels to law enforcement agencies for urgent threats.
- Compliance with local regulations and protocols for handling and reporting child exploitation and abuse.
- Secure data sharing mechanisms to provide necessary information to authorities.

3.4.7. Incident Response Teams:

ISP's should establish dedicated teams to handle and respond to reported incidents. The team should include:

- Trained professionals who specialize in online safety and incident response.
- Clear protocols for assessing and escalating reported issues.
- Collaboration with cybersecurity experts for technical investigations.

3.5. Collaboration with Law Enforcement:

3.5.1. Establish Clear Reporting Protocols:

ISP should develop clear and efficient protocols for reporting incidents to law enforcement. This protocol should include:

- Define the types of incidents that require law enforcement notification, such as child exploitation, cyberbullying, and threats of violence.
- Standardize procedures for reporting incidents, including the necessary information and documentation.
- Ensure quick and secure transmission of reports to relevant authorities.

3.5.2. Dedicated Contact Points:

ISP's should designate dedicated contact points within the ISP and law enforcement agencies. They should:

- Appoint specific individuals or teams responsible for coordinating with law enforcement.
- Establish direct communication lines, such as dedicated phone numbers and email addresses.
- Maintain updated contact lists for relevant law enforcement personnel.

3.5.3. Regular Communication and Coordination:

ISP's should foster ongoing communication and coordination between ISPs and law enforcement. They should:

- Schedule regular meetings and briefings to discuss emerging threats, trends, and collaborative efforts.
- Participate in joint task forces and working groups focused on

online child safety.

- Share updates on new technologies, policies, and best practices.

3.5.4. Training and Awareness Programs:

ISP should collaborate on training and awareness programs to enhance the capabilities of both ISP staff and law enforcement. They should:

- Conduct joint training sessions on recognizing and responding to online threats against children.
- Share educational resources and materials on the latest cyber threats and safety measures.
- Provide ISP staff with knowledge on legal requirements and procedures for working with law enforcement.

3.5.5. Incident Response Collaboration:

ISP should work together on incident response to ensure swift and effective action. They should:

- Develop joint response plans for various types of incidents, including cyberbullying, exploitation, and threats.
- Coordinate actions during incidents, such as evidence collection, suspect identification, and victim support.
- Ensure clear communication and role definition during incident response.

3.5.6. Legal Compliance and Advocacy:

ISP should ensure compliance with legal obligations and advocate for policies that enhance child safety online. They should:

- Be informed about laws and regulations related to child protection

and online safety.

- Advocate for stronger laws and policies to protect children from online threats.
- Collaborate with lawmakers and regulatory bodies to develop effective legal frameworks.

3.5.7. Crisis Management and Support Services:

ISP should provide coordinated crisis management and support services for victims of online threats. They should:

- Offer immediate support and resources for victims and their families, in collaboration with law enforcement and victim support organizations.
- Ensure that victims have access to assistance, and other necessary services.
- Develop and maintain protocols for handling crisis situations, including public communication strategies.

3.6. Encrypted Connections:

3.6.1. HTTPS Everywhere:

ISP should ensure that all websites and services accessed via the ISP's network use HTTPS (Hypertext Transfer Protocol Secure). There should be features for:

- Automatic redirection from HTTP to HTTPS for all web traffic.
- Encourage and support website operators to adopt HTTPS by providing resources and assistance.
- Monitor network traffic to identify and address any instances where HTTPS is not being used.

3.6.2. Secure Email Services:

ISP should offer secure email services that use encryption to protect email content. There should be features to:

- Ensure end-to-end encryption for emails sent between users on the same service.
- Support for encrypted email protocols such as PGP (Pretty Good Privacy) or S/MIME (Secure/Multipurpose Internet Mail Extensions).
- Provide easy-to-follow instructions for customers to set up and use encrypted email.

3.6.3. Secure Cloud Storage:

ISP's should offer secure cloud storage solutions with encryption for data at rest and in transit. There should be features:

- Use strong encryption protocols (e.g., AES-256) for all data stored in the cloud.
- Provide features such as two-factor authentication (2FA) and secure file sharing.
- Educate customers about best practices for using cloud storage securely.

3.6.4. Secure Browsers and Extensions:

ISP should encourage the use of secure web browsers and extensions that enhance privacy and security. They should:

- Promote the use of browser extensions that enforce HTTPS, block trackers, and enhance privacy (e.g., HTTPS Everywhere, Privacy Badger).
- Provide guidance on configuring browsers for maximum security.

3.6.5. Encrypted Backups:

ISP should provide encrypted backup solutions to protect data from unauthorized access. There should features that:

- Ensure that all backup data is encrypted both in transit and at rest.
- Offer automated and user-friendly backup services with strong encryption.
- Educate customers about the importance of regular backups and secure storage.

3.7. Search Filters:

Safe search filters are crucial tools that ISPs can implement to ensure child safety online by blocking inappropriate content and providing a safer browsing experience. Here are the key safe search filters and related measures that ISPs can implement:

3.7.1. Parental Control Dashboards:

ISP should provide user-friendly parental control dashboards for managing safe search settings and monitoring activity. There should have features to:

- Allow parents to view and adjust safe search settings for all devices connected to their home network.
- Provide activity logs and reports showing search queries and attempts to access blocked content.

3.7.2. Content Review and Whitelisting:

ISP can implement content review mechanisms and allow parents to whitelist safe websites. They should have features to:

- Provide a feature for parents to manually review and approve websites for their children.

- Maintain a whitelist of approved educational and child-friendly websites.

3.8. Community Engagement:

Community engagement is a vital aspect of ensuring child safety online. ISPs can play a proactive role in fostering a safe online environment by engaging with the community, raising awareness, and collaborating with various stakeholders. Here are the key community engagement measures that ISPs can implement to enhance online child safety:

3.8.1. Community Partnerships:

ISP's should partner with content providers, platforms, local organizations, non-profits, and law enforcement agencies to promote child safety. They should ensure mechanism to:

- Work with child protection agencies and advocacy groups to develop and implement safety initiatives.
- Participate in community events and fairs to distribute educational materials and provide information on online safety.

3.8.2. Interactive Online Resources:

ISP should develop and maintain a dedicated online safety portal with resources for parents, children, and educators. There should be features to:

- Provide interactive tools such as quizzes, games, and tutorials to educate children about safe online behavior.
- Offer downloadable guides, checklists, and templates for parents and educators to use in teaching online safety.

3.8.3. Safe Online Behavior Pledge:

ISP's should introduce a safe online behavior pledge that families can commit to. They should:

- Encourage families to sign a pledge that outlines commitments to safe and responsible internet use.
- Provide certificates or digital badges for families that participate, promoting a culture of safety and responsibility.

3.8.4. Regular Surveys and Feedback Mechanisms:

ISP's should conduct regular surveys and feedback sessions to understand community concerns and improve safety measures. They should:

- Use surveys to gather insights on the effectiveness of current safety initiatives and identify areas for improvement.
- Hold focus groups and community meetings to discuss online safety issues and gather direct feedback from parents and children.

3.9. Documentation:

3.9.1. Documentation Measures:

3.9.1.1. Detailed User Manuals and Guides:

ISP's should provide comprehensive manuals and guides for setting up and using parental controls and other safety features. There should feature to:

- Include step-by-step instructions, screenshots, and troubleshooting tips.
- Offer both digital and printable versions for accessibility.

3.9.1.2. Frequently Asked Questions (FAQs):

ISP's should maintain a well-organized FAQ section on the ISP's website covering common safety concerns and solutions. There should features to:

- Regularly update with new questions and solutions based on user feedback.
- Ensure easy navigation and search functionality.

3.9.1.3. Online Safety Resource Center:

ISP's should create a dedicated section on the ISP's website focused on online child safety resources. There should be features to:

- Provide articles, videos, infographics, and links to external resources about online safety.
- Offer downloadable content such as checklists and activity guides for parents and children.

3.9.1.4. Policy Documents:

ISP's should develop and publish clear policy documents outlining the ISP's commitment to child safety online. There should be feature to:

- Include privacy policies, terms of service, and safety guidelines.
- Make documents easily accessible and understandable for all users.

3.9.1.5. Regular Newsletters and Updates:

ISP's should send regular newsletters to users with updates on new safety features, tips, and best practices. There should be features to:

- Highlight recent changes, upcoming features, and relevant news about online safety.
- Include sections for user stories, expert advice, and community feedback.

4. COMPLIANCE:

Ensuring child safety online requires ISPs to comply with a variety of legal, regulatory, and industry standards. These compliance measures help protect children from online harm and ensure that ISPs adhere to best practices and legal requirements. Here are key compliance measures that ISPs should implement:

4.1. Adherence to Legal and Regulatory Requirements:

ISP's should comply with all relevant national and international laws regarding online child protection. ISP's should adhere to:

- Online Child Safety Directives (2019): These directives aim to protect children from online abuse and harm by setting guidelines for internet use.
- Guidelines for Parents, Guardians, and Educators on Child Online Protection: Issued by the Nepal Telecommunications Authority, these guidelines provide advice on reducing online risks for children.
- Children's Act (2018), Electronic Transactions Act (2008), and Criminal Code (2017): These laws encompass various aspects of online safety and cybercrime.
- Bylaws and directives issued by the regulator Nepal Telecommunications Authority : Cyber Security Bylaw (2020), Internet Service Regulation Bylaw (2020), Online Child Protection Directives (2019).

4.2. Development and Enforcement of Acceptable Use Policies (AUP):

ISP's should create and enforce clear Acceptable Use Policies that outline prohibited activities and consequences for violations. They should:

- Define inappropriate content and behavior, including bullying, harassment, and accessing adult content.

- Communicate AUP to all users and ensure acknowledgment of terms during account creation.

4.3. Data Protection and Privacy Policies:

ISP's should implement stringent data protection and privacy policies to safeguard children's personal information. They should:

- Ensure compliance with data protection laws.
- Limit the collection, storage, and sharing of children's data and ensure secure handling.

5. REVIEW AND REVISION

Version Number	Date	Author	Description of Changes	Reviewer	Approval Date	Notes
1.0	2024-06-01	Suvash Khadka	Initial version was created	Mr. Kapil Aryal, Mr. Aavash Khadka, Mr. Ram Krishna Pariyar	2024-06-18	Initial submission
1.1	2024-06-30	Suvash Khadka	Final version created	Mr. Aavash Khadka, Mr. Ram Krishna Pariyar, Mr. Santosh Maharjan.	2024-11-19	Final submission (incorporating feedback received on 'Consultative Workshop on SOP for Internet Service Providers' at Bogini Nagarkot Resort, Nagarkot).