Guidelines for Protecting Children on the Internet

Ministry of Transport, Communications and Information Technology

General Directorate of Policies and Governance

2021

Approval and Distribution:

	Name	Email	Issuance Date
Issuance Authority	General Directorate of Policies and Governance	Covernance@mtcit.gov.om	2021
Reviewed by			
Approved by			

Distribution List:

1	
2	
3	

Document Review Record:

Version	Date	Issuing Authority	Notes
0.1	2021	General directorate of policies and Governance	Creating the Document

Table of Contents

1. Introduction:

Over the past ten years, the usage and role of the Internet have significantly changed in the life of lots of people. The number of users who can access the Internet is continuously increasing with the spread of smartphones and tablets, the developments in social media platforms and applications as well as accessibility to communication technologies such as Wi-Fi, 4G and 5G networks. In addition, the novel International Coronavirus Pandemic (COVID-19) witnessed an increase in the number of children who, for the first time, joined the Internet world to complete their studies and interact on social media platforms. The exceptional conditions that were produced by the pandemic and its accompanying challenges made many younger children interact online much earlier than their parents had planned.

Although Information and Communication Technology provides children with many opportunities for communication, learning new skills, and creativity, it also may constitute potential risks to children's safety such as privacy, cyberstalking, cyber blackmail, the misuse of personal data and other issues.

2. Document Objective:

This Document aims to develop guidelines for policymakers, Information and Communication Technology service providers, parents, educators and care providers to confront all potential threats and damages that may face children online.

3. Target Audiences:

- Makers of policies related to children's rights in the Sultanate.
- Parents, educators and care providers in the Sultanate.
- Information and Communication Technology Services providers in the Sultanate (communication services providers, archived digital content service providers, connectivity services and data storing and hosting suppliers, user-generated content services suppliers, and systems based on Artificial Intelligence providers).

4. Definitions and Terms:

Child	Any person who is less than eighteen calendar years.
Protecting Children on the Internet	Adopting a comprehensive approach to building safe digital spaces that is appropriate for age, comprehensive and sharing for children including response, support, and self-help to face threats, prevent damage and achieve balance between guaranteeing protection and providing children with opportunities to be digital citizens and uphold the rights and duties of both children and society.
Care provider	The person who is responsible for taking care of, raising and growing the child such as the custodian, guardian and the entity entrusted with that.
Educator	The role of educators includes those who teach in classrooms and other persons who perform an unofficial role in the educational process.
Digital Citizenship	It is the ability to engage positively in the digital environment depending on the skills of the responsible usage of technology and effective communication of practicing the forms of social participation that respect human rights and dignity through the responsible usage of technology.
Information and Communication Technology	All information technologies that depend on communications including all services and devices connected to the Internet such as computers, laptops, tablets, smartphones, game consoles, and smartwatches. They also include services such as radio and television as well as broadband services, networking hardware and satellite systems.

Personal Data	Data that directly or indirectly makes a natural person identified or identifiable by referring to one or more identifiers such as the name, civil identity number or website data, or by referring to one or more factors related to genetic, physical, mental, psychological, social, cultural or economic identity.
Parental Control Tools	Software that enables users who are usually one of the parents to control some or all functions of the computer or any other device that can be connected to the Internet. This software can limit access to certain types or categories of websites or services on the internet. Some software also enables the ability of time management to set the device access to the Internet in certain hours exclusively. More advanced versions can record all sent and received texts from and to the device and the programs are usually protected with a password.
Online Games	Any type of single or multi-player commercial digital gaming via any device connected to the Internet including custom consoles, desktop computers, laptops, tablets and cell phones.

5. Classification of Major Threats that Children are Exposed to on the Internet:

Information Fatigue Syndorme	It means that the child is frequently exposed to inaccurate or incomplete information without verifying its validity because of using the Internet without control.
Cyberstalking	It describes a deliberate aggressive act frequently executed by a group or one person by using digital technology to target a victim who cannot defend himself easily, such as posting harmful information about someone, sharing private information, pictures, or videos intentionally and harmfully, sending threatening or offensive messages (via email, instant messaging, or chat), or spreading rumors and false information about the victim.
Cyber Blackmail	It is carried out by using modern technology to threaten and frighten the victim by posting pictures or releasing personal information about him to get material or moral gains. Victims are usually hunted via email or different social media programs due to their widespread and large use by all society groups.
Cyberbullying	Exposing children to mocking in mutual talks on social media platforms or in online games. This also includes exposing children or "their characters in games" to continuous attacks.
Personal Data Violation and Misuse	Posting information that identifies personal identity without realizing it, such as posting personal information in personal profiles on social media sites identifying addresses or geographic locations on maps, or opening webcams in devices.
Phishing	Using email and SMS for deceiving people into clicking malicious links or attachments. Sites that are popular among children can be used to collect email addresses and friends' names to use them in deceptive messages.

Falling for scams	Deceptive messages provide things that can be obtained as a prize such as free access to online games in return for providing some important information such as the parents' credit card information.
Undesirable Advertisements	Some companies send spam messages to children via websites to sell their products.
Downloading malware unintentionally	Using technology to deceive people into downloading malware such as convincing victims to download fake games that can be deceptive for children in particular. Malware may contain several functions such as spying and stealing the user's information (passwords and pictures) to use them to send spam or carry out cyber attacks on other parties, take stolen files hostage and demand ransom, or just destroy the operating system.
Defamation and Reputation Damage	Editing photos and videos offensively and posting them on the Internet which results in bad comments, reputation damage and defamation.
Access to inappropriate content, goods and services	Exposure to inappropriate or even criminal content may lead children to extremism such as self-harm and destructive and violent behavior. Exposure to such content may also lead to embracing racial or discriminatory thoughts.
Dangerous Conversations	Exploiting communication channels via emails, instant messages, or social networking by anonymous people to chat with children by using their accounts on digital platforms and social media in a manner that exposes them to danger.

6. General Guidelines:

6.1 Guidelines for Policymakers:

To guarantee the protection of children on the Internet, Policymakers related to children's rights must consider a package of key fields including:

1. Reviewing the current legal framework and developing comprehensive regulatory frameworks and policies to guarantee the protection of children on the Internet.
2. Engaging all stakeholders concerned with children's safety on the Internet to formulate and implement a national initiative that focuses on converting the Internet into a safe place for children and young people. In addition, Raises awareness on the included issues in the initiative and how to practically address them.
3. Establishing and broadly diffusing an easy and applicable mechanism for reporting harmful content on the Internet.
4. Ensuring the existence of international and methodological mechanisms to protect children- including children with disabilities- that oblige all those who work with children (authorities concerned with health, social care and schools) to identify, handle and report abuses and damages that occur on the Internet.
5. Developing the skills of being aware of digital knowledge as a part of any national school curriculum so that it can be appropriate for the children's age and applicable to all children.
6. Organizing national awareness initiatives to shed light on the issues of children's protection on the Internet at both the local and international levels.
7. Conducting research at the national level by all stakeholders concerned with children's safety concerning the protection of children on the Internet.

6.2 Guidelines for Parents, Educators and Care Providers

Guidelines for Parents and Care Providers:

1. Enhancing children's confidence through conversation and exchanging digital experiences with them regarding their online activities.
2. Identifying technologies and devices used by family members including children and identifying online services as well as applications in all these devices.
3. Ensuring the installation and continuous update of firewall software and antivirus software in all the devices used in the house and ensuring that this software is important to support parental control systems on the Internet.
4. Teaching children the basics of Internet security including systems and applications and ensuring that they are updated, in addition to strengthening the culture of asking for support and assistance from parents when they are facing online risks.
5. Setting rules for using the Internet and personal devices, taking into consideration privacy-related matters, inappropriate websites, applications and games, time taken in front of the screen and other risks represented by strangers.
6. Parents must know about services used by children on the Internet such as social media platforms, websites, applications, games and others.
7. Sufficient knowledge of how to report risks on platforms used by children and how to delete profiles or edit them, in addition to training children on that.
8. Educating children on information that must be kept confidential when using online applications and services.

Guidelines for Educators:

1. Develop a school policy to organize where and how to use the technology inside the school by different stakeholders, in addition to how to manage incidents of children protection.
2. Ensure the safety of the school network and devices by securing them using a password and installing antivirus and firewall software.
3. Ensure that the Internet content provided by the school is subject to sorting and control, in addition to reviewing online safety measures regularly.
4. Ensure that the school management team is sufficiently aware of online safety at school.
5. Comply with online professional communication with students, parents, and other stakeholders via the school email, in addition to prohibiting individual digital contact with students and any other contact that is not for educational purposes or via non-school platforms. In addition, personal accounts are not allowed for communicating with students or parents.
6. Contribute to the development of the students' digital skills and digital literacy.
7. Identify an employee as a contact point at school to collect and record events related to online safety
8. Ensure that all employees at schools (including support employees) have got sufficient training to address risks that may be faced by students on the Internet and regularly enhance their skills.
9. Estimate educational and psychological effects that may be caused to children by the Internet and online communication technology.

6.3 General Guidelines for Information and Communication Services Providers:

The Information and Communication Services Providers can identify and mitigate the harmful effects of Information and Communication Technology on children and identify the opportunities provided to them to support upgrading children's rights in the digital world through the following guidelines:

1. **Integrate considerations of children's rights into all policies and administrative processes of service providers**:
    - Develop a policy for children's protection as well as integrate risks and opportunities related to children's rights into the obligations of the Service provider's general policies (such as user's rights, privacy, marketing and relevant codes of conduct).
    - Establish mechanisms for grievance and reporting any violations of children's rights such as content harmful to children and violation of privacy.
    - Develop policies to protect children who contribute to online content by participating in programs, films, games, news and other content.
    - Approve policies related to the ownership of content created by users such as the nature of the service, what is expected from its users, and accepted or unaccepted content/ behavior or language/ consequences resulting from the violation including removing the content that violates the service provider's policy.
    - Enhance the benefits of Artificial Intelligence technologies by the service provider to protect children online.
    - Adopt an approach to engage a large group of stakeholders such as parents, teachers and psychologists specialized in children- and children themselves if needed- when developing products and services targeting children.

2. **Set standard rules to address content harmful to children**:
    - Cooperate with law enforcement and civil society institutions to effectively deal with the content harmful to children and report to the competent authorities.
    - Conditions of Service must explicitly clarify the service provider's stand on the misuse of its services to store or share material or content that is harmful to children and the consequences of that.
    - Establish a clear and easy mechanism to report content harmful to children including information and instructions to users about the approach to be adopted.
    - Service Conditions and Terms must state that in the event of discovering and reporting materials or content harmful to children, the service provider shall completely cooperate with the law enforcement Authorities.

- Document the service provider's practices to deal with content harmful to children starting from supervision to removing and completely disposing of the content, in addition to including a list of all employees in charge of that.
- The contract between the service provider and other parties must include setting rules and conditions to deal with content harmful to children and reporting cases to the competent authorities.
- Include and maintain Data Retention Policies to support law enforcement in the event of carrying out criminal investigations, in addition to collecting evidence and not destroying it except after coordination with the Law Enforcement Authority.
- Conduct an assessment regularly of all content hosted by the service provider's servers, including commercial content provided by third parties.
- Prevent pre-access to web addresses containing content that is not suitable for a wide audience, as well as block access to content that is harmful to children.

3. **Prepare a safer digital environment that is appropriate for the age factor**:
    - Establish technical controls that are easy for users to apply and provide the capability to block or filter access to the Internet via the service provider's networks.
    - Work with the concerned authorities to develop content classification systems according to age based on national or international standards.
    - Display the report feature on all web pages and services in addition to developing and documenting clear processes to manage harmful content or other violations of conditions and terms.
    - Approve suitable mechanisms to verify age to prevent children from accessing content, sites, products or interactive services that take age into consideration.
    - Provide advice and notifications to users regarding the nature of the content they use and classify it according to age.
    - Provide a personal identification number by providers of online audio, visual and multi-media services to users who seek to access content that may be harmful to children.
    - Ensure that data collection policies comply with relevant laws related to privacy and children's protection.

- Develop and include policies suitable for online advertisements targeting children in an easy language for users to understand in the service conditions and usage instructions such as content that supports interactive factors such as commenting on online forums, social networking, games platforms or chatrooms.
- Include statements in the use conditions and terms to prevent using other Wi-Fi networks to access or display any materials that may be inappropriate in an environment where there are children. Terms and conditions should also contain clear mechanisms with regard to the consequences of violating these rules.
- Taking all necessary measures for protection from unauthorized access that may lead to manipulating or losing personal data.
- Provide procedures and software for guidance and enable optional parental control related to children's access to online content.
- Access Wi-Fi networks is identified via SIM individual cards or other identifiers.
- Consider the age of digital approval that includes requesting the parents' approval before allowing new users to use or participate in websites that include children's content.
- Provide settings of age-appropriate content sharing and visibility, such as making children's privacy settings more restrictive by default than adult settings.
- Protect younger users from unsolicited communication and ensure that there are guidelines concerning privacy and data collection.
- Place restrictions on the collection, processing, storage, sale and dissemination of children's personal data using Artificial Intelligence technologies by the service provider.

4. **Educate children, educators and care providers on children's safety and the responsible use of Information and Communication technology:**
    - Provide users with clearly specified information on the content such as content type, age classifications, restrictions, available parental control tools and how to report misuse and harmful content.
    - Encourage adults, particularly parents, care providers and educators to participate in using the content available for children on the internet in order to be capable of helping and directing children to choose the content that suits them and assist in setting the code of conduct.
    - Provide the rules of usage in a clear and easy language that encourages children to be careful and responsible when browsing the internet.
    - Establish tools appropriate for age such as educational courses and help centers, in addition to providing a contact link with a helpline or consultation service.
    - When online content is likely to attract a high percentage of children, make safety information in the form of prominent, user-friendly and clear links and icons.
    - Provide a tool to direct parents to control content that can be accessed through a certain browser.
    - Cooperate with parents to ensure that information revealed online regarding children does not expose them to danger.
    - Where possible, obtain children's prior consent when showing them on the internet in programs, films, videos, etc and respect any refusal to participate.
    - Provide parents with clear information about available content and services, including for example an explanation of social networking sites and services on the site, how to access the Internet using portable devices, and options available for parents to apply controls.
    - Acquaint parents with how to report misuse and harmful content and inform them about age-restricted services and other ways to act safely and responsibly when using interactive services.

- Provide advice as well as notifications about the nature of a certain service or content and how to use it safely.
- Develop social guidelines in interactive services, such as safety-related pop-ups that remind users of proper and safe behavior such as not disclosing their contact details.
- Inform users including children, their parents and care providers about Artificial Intelligence Platforms to enable them to make decisions on using or refusing these platforms.

5. **Enhance Digital Technology as a means of increasing civil participation:**
    - Develop or provide a set of high-quality and attention-attracting educational content that suits age.
    - Encourage content that enables children to build their abilities and skills in addition to set a positive role model by providing new opportunities for entertainment and education contributing to their physical, mental and social growth.

6. **Use technological progress to protect children:**
    - Invest in developing systems based on artificial intelligence to detect acts of child abuse and bullying via the Internet, in cooperation with agencies related to children's rights.

7. **References:**

- Omani Child Law issued by Royal Decree No. (22/2014)
- Law On Juvenile Accountability issued by Royal Decree No. (30/2008)
- UNICEF Report on Children's Rights and Online Games (2019).
- UNICEF Report on Artificial Intelligence and Children's Rights (2018).
- International Telecommunication Union Report on Digital Citizenship Education (2019)
- UNICEF Report on Children in the Age of the Web (2017).
- UNICEF Report on New Technology and 21st Century Children.
- UNICEF Report on Building Resilience for Children via the Internet (2014)