

# SAFEGUARDING YOUR CHILD IN THE DIGITAL AGE

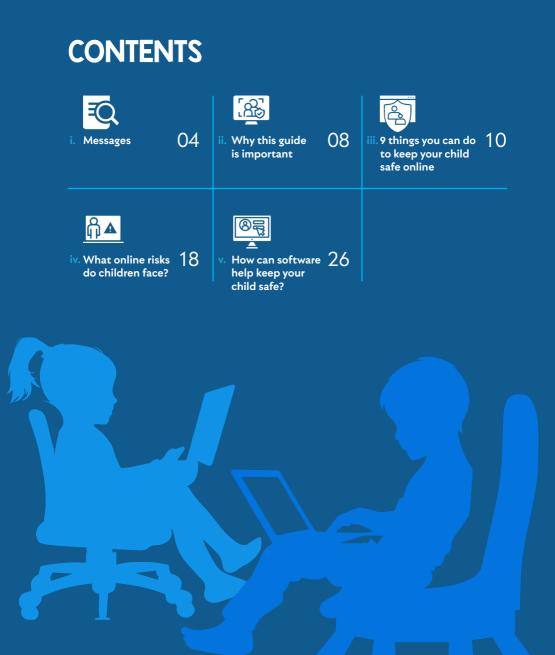
A guide for parents and caregivers







Designed by **HUMAN** Design Studios



### MESSAGE FROM CHAIRMAN, PTA



Major General (R) Hafeez Ur Rehman, HI (M)

I am pleased to introduce to you this guide on Child Online Safety, meticulously prepared by the Pakistan Telecommunication Authority (PTA) in collaboration with UNICEF and Telenor. In this age of technology, children have an unprecedented level of access to information, people and entertainment in the cyber world. It is therefore imperative we make ourselves ready for challenges to come. This guidebook will equip parents and caregivers with the latest knowledge and tools to ensure the safety and wellbeing of their children online while meeting their educational needs.

PTA is well aware that child online protection is a global challenge and cannot be effectively handled without national and international cooperation. PTA's continued efforts to meet this global challenge were receipt recognized on the international stage through the SAMENA Council international LEAD award for enabling child and youth safety online. However, the journey towards a truly safe and secure online environment for children has only just begun. The role of parents and caregivers is of paramount importance throughout this journey. We (parents) needs to spare time for their kids, prove ourselves a good online role model and build trust among children by promoting open communication.

I extend my heartfelt appreciation to Muhammad Farooq, Head of PTA's Child Online Protection committee and his team for their dedication in preparing this informative toolkit. While we acknowledge that parents know what's best for their children, I am confident that this guidebook will be an invaluable resource to they keep their children protected in cyberspace.

Thank you for your commitment to the well-being of our youth in the digital age.

### MESSAGE FROM UNICEF COUNTRY REPRESENTATIVE



Abdullah A. Fadil UNICEF Representative in Pakistan

The world in which our children are growing up looks vastly different from the one we, as their parents, experienced. They now have access to an unprecedented range of technologies and information, thanks to connectivity. This has brought opportunities for even the most marginalized children to acquire knowledge, fulfill their educational potential and engage in civic participation.

However, alongside these opportunities, significant risks emerge. As parents and caregivers, it is our responsibility to help children navigate this new world, ensuring they maximize the benefits while being protected from the risks. These dangers include sexual exploitation and abuse, bullying, as well as exposure to misinformation that could potentially lead to violence and hatred.

UNICEF actively supports children in safely navigating the online spaces. Acknowledging that digital technology can increase exposure to harmful materials and behaviours, UNICEF is pleased to have been able to contribute technically to this guide, conceptualized by PTA, along with other partners, namely NCRC and Telenor Pakistan. The guide aims to help parents and caregivers understand the types of risks that children face in the digital age, and points to tools and techniques to safeguard against these risks. It underscores the importance of positive parenting, trust and open communication so children are empowered to learn and develop their full potential while being protected from violence, exploitation and abuse - whether online or offline. The guide intends to equip today's parents with necessary guidance and tools in our rapidly evolving world.

### MESSAGE FROM CHAIRPERSON, NATIONAL COMMISSION ON THE RIGHTS OF THE CHILD



Ayesha Raza Farooq

In this rapidly evolving digital age, our children are navigating a world filled with endless possibilities and opportunities. However, along with these advancements come significant challenges and risks that can impact their safety and well-being.

As Chairperson of the National Commission on the Rights of Child (NCRC), I am deeply committed to ensuring the protection and well-being of the more than 102 million children in Pakistan. It is our collective responsibility to equip our children with the necessary tools and knowledge to thrive in this digital landscape while safeguarding them from potential harm.

I am pleased to introduce this guide developed by PTA, to which UNICEF has made technical contributions in collaboration with Telenor and NCRC. It aims at empowering parents and caregivers with valuable insights and strategies to navigate the digital world responsibly.

By raising awareness among parents, caregivers and educators on digital safety, we can support them to create conducive environment for children to explore, learn, and grow while staying safe from online threats such as cyberbullying, exploitation, and misinformation. MESSAGE FROM CEO, TELENOR, PAKISTAN



Khurrum Ashfaque

As a father of three, I constantly reflect on the balance between the advantages and risks that technology brings into our lives. The internet is a fantastic resource for children and young people, providing them with opportunities to learn, share and connect with the world. However, it can also present them with challenging situations, such as exposure to harmful content, bullying, grooming and scams.

At Telenor, we want to help today's young people become more confident and resilient when they're online. We share this responsibility and have partnered with UNICEF and PTA to produce a guide aimed at helping you understand the main risks children face in the digital age. It offers practical tools and techniques to safeguard against these risks, emphasizing positive parenting, trust, and open communication.

Let's set out on this journey together, creating a digital environment that protects and nurtures the unique potential of our children. In our roles as parents, caregivers and teachers, our commitment is the key to making the online world a secure space for the dreams and aspirations of our youth.

Thank you for entrusting us with this shared responsibility.

A Guide Book for Parents: To keep Children Safe from Online risks

# ii. WHY THIS GUIDE IS IMPORTANT



The internet is an unprecedented source of information, entertainment and educational content for children and young people. Despite its benefits, the internet also exposes children to new threats, and unlawful online activities and crimes are on the rise. Yet, many parents and caregivers do not realize the types of online risks to which children may be exposed.

As a parent or caregiver, you need to be equipped to guide children on using the internet safely and responsibly in a healthy online environment.

By building a thorough knowledge of online risks and learning how to use

safety measures, you can protect children and guide them on how to respond effectively to potential online dangers.

This guide was initially conceptualised and designed bv Pakistan Telecommunication Authority (PTA). It received technical contributions from the United Nations Children's Fund (UNICEF) Pakistan and HQ, Telenor and feedback from the National Commission on the Rights of the Child (NCRC). It has been developed to equip you, as a parent or caregiver, with the knowledge and tools to ensure your children use the internet safely and responsibly



#### **PTA EXPLAINS:**

Keeping children safe online: The role of parents and teachers https://www.youtube.com/watch?v=eQ-Almqu0c4&t=2s

#### **REMEMBER:**

Pakistan Telecommunication Authority is committed to empower parents, caregivers and children with the knowledge and skills needed to navigate the internet safely and wisely

# iii.9 THINGS YOU CAN DO TO KEEP YOUR CHILD SAFE ONLINE

#### 1. Be a good online role model for your children

Children often do what they see their parents doing. You are a role model for your child(ren), and your actions can have a deeper influence on them than words or digital tools.

You should set a positive example for your children and demonstrate responsible online behaviour to navigate the digital world safely and responsibly. This means interacting online respectfully and positively with others in digital spaces, and avoiding illegal or unethical behaviours online. Just because it's online doesn't mean there are no consequences!

Seek out reliable resources, including from UNICEF and PTA, on the latest issues in keeping children safe online, and to report inappropriate online content.





#### **PTA EXPLAINS:**

Safe and responsible social media use in Pakistan https://www.youtube.com/watch?v=PrtzTyB8nlk

#### 2. Build trust and communicate openly

Parents should make sure they understand new technologies and how these are used by their children. You should spare time to talk to your child, listen respectfully to their views and keep an eye on warning signals.

encouraging

communication and creating a home environment where children feel free to discuss bad experiences, concerns or problems they face when online.

It's better to start conversations about online hazards at an early age and educate children about online harm.

open

#### **REMEMBER:**

This

means

children may be more knowledgeable about the online world than you! You can also learn from your children. This will help you build trust and stay informed about your child's online activities and experiences and to act quickly if preventive measures are needed.

#### 3. Don't blame your child for their negative online experiences



Bad online experiences can have severe impacts on children's wellbeing,

health and safety. But by supporting your child, listening to their concerns and believing what they tell you, you can create a nurturing and supportive environment in which they will flourish. If a child knows that you will not blame them, they are more likely to tell you if they are worried about any online experiences, so you can act to safeguard them.

## 4. Teach your child how to recognize and respond to inappropriate online behaviour

Teach your child to be wary of anyone, even someone they know, asking too many questions about their personal life or family, requesting photographs, or asking inappropriate questions about their body. Make sure your child knows what information is private, such as their full name and school, contact information, personal photos, and the personal information of their family members. They should never share passwords or give other people access to their online accounts, not even their closest friends.

Teach your child that it's all right to refuse to answer if someone who is

not a trusted adult asks for private information. Teach them it's ok to say *no!* in such settings.



#### 5. Set clear ground rules for internet use

Make sure your children know how to be responsible internet and social media users. Ensure they know that discriminatory, inappropriate or bullying behaviour is never acceptable, and that anything they post online will leave digital footprints.

Together with your child, establish rules on how, when and where to use internet devices and for how long. Avoid giving handheld devices like mobile phones to very young children. You might prefer that they only use electronic devices in family areas and at specific times, so that you can keep an eye on their online activities and limit excessive screen time.



#### 6. Encourage critical thinking

No parent or caregiver can protect children from every hazard. It's best to empower children to protect themselves through the power of critical thinking, so they can respond to situations as they arise.



Equip your child with media literacy and decision-making skills, and encourage them to seek evidence and ask questions. This will not only guide them to take the right decisions online, it is an invaluable skill for flourishing at school and at work.

Thinking critically about their

interactions can help children recognize online threats such as potentially harmful interactions. Be cautious about free online resources, even educational ones, as they sometimes collect private information. If your child is asked to provide a photo or their full name, be sure it is a trusted website.

#### 7. Encourage a healthy balance between online and offline activity



Spending time on the internet, using social media and playing games can be energizing and healthy for a child! The internet gives opportunities for a child to learn, be creative and share their views. At the same time, encourage children, both girls and boys, to take part in ageappropriate physical activities so they have a healthy balance between screen time and offline activity. They can also make use of valuable online resources for offline life, like exercise videos.

#### 8. Use the technological tools available to keep your children safe

While no parent or caregiver can rely on technological tools alone, parental control tools developed by software and social media companies can help you oversee your child's digital activities, especially for younger children. By knowing which parental controls exist and how they should be used, you can shape a virtual environment in which your child can safely explore and learn.

Make sure that the device your child uses is always updated and running the latest software, and that privacy settings are on and configured to minimize data collection.

Help your child learn to keep personal information private. If your privacy settings are not secure, anyone can see your information. Similarly, it's important to keep your passwords private and never share accounts, even with your closest friends.

You or your child can always call 1121 for advice on any concerns related to child protection, report harmful online content to PTA and FIA, or reach out to NCRC to register a complaint.



But always remember – technology is not enough. A nurturing and supportive relationship with your child will ultimately have a huge impact on their safety.

#### 9. Empower your child to stand up to peer pressure



Children often come under pressure from friends to join social media or engage in online activities even when they are too young or not interested. Children may even be pressured to join in joking and teasing that can be harmful or painful to others. Guide your child from an early stage that they can always refuse to participate in activities they are uncomfortable with.

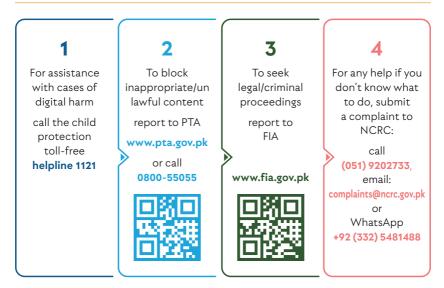
Most importantly, teach your child about keeping themselves and others safe, the core values of politeness and mutual respect, and boost their confidence, critical thinking and selfesteem to cope with peer pressure.



#### **PTA EXPLAINS:**

How to file a complaint with PTA – by phone or online <a href="https://www.youtube.com/watch?v=UCFwoeAnzE0">https://www.youtube.com/watch?v=UCFwoeAnzE0</a>

#### Get help against online risks



# iv.WHAT ONLINE RISKS DO CHILDREN FACE?



#### Child online sexual abuse and exploitation

Many forms of child sexual abuse and exploitation are facilitated or enabled by digital technology.

People wishing to harm children often try to get close to them over the internet by taking advantage of their innocence and lack of adult supervision. They often use social media and gaming platforms to gain a child's trust and then exploit this trust.

Often, children do not understand why it is important to keep personal information private, such as their name, their school, and photos of themselves or their families. Sharing such information, especially with strangers, can make them and your family vulnerable to scammers, hackers and even sexual predators.

When people befriend a child online with the intention of exploiting them through sexual abuse, it is known as "grooming". These sexual predators and groomers are not always strangers: they can even be people the child already knows.



Sexual abuse can be in person or online. It can include having ageinappropriate discussions with children, or even obtaining sexually explicit images and videos of the child that could be used to produce or sell child sexual abuse materials.

## What can I do if I think my child is being targeted for child online sexual abuse and exploitation?

- Teach your child how to say no! if they feel uncomfortable or unsafe in any situation.
- Do not blame the child and ensure that your child understands you will believe and protect them.
- Reassure the child that experiencing abuse or harassment is never their fault.
- Make the child's accounts private so others cannot view them.
- Educate your child about the

importance of online safety and privacy and never giving out information about themselves and their family online.

- Create an open dialogue with your child about healthy relationships, and help children recognize the warning signs of predatory or harmful behaviours.
- Call the child protection helpline 1121 for assistance, report the issue to PTA and FIA or register a complaint with NCRC.

#### Cyberbullying

When a person uses digital technology to deliberately and repeatedly harass, humiliate, embarrass, torment, threaten, pick on or intimidate another person, it is known as cyberbullying.

While friends often joke together, sometimes the joke goes too far and leaves someone feeling hurt and upset. When this happens online, then it is a form of cyberbullying.



#### Cyberbullying can include:

- posting or sending threatening messages
- creating unkind or unpleasant fake social media accounts using someone else's actual photos or contact details without their consent
- sharing or forwarding people's personal information without their permission
- posting insulting or embarrassing photos or videos of people without their permission
- spreading lies about someone online

Cyberbullying can take place through many different channels, including text messages, emails, online games and social media platforms. It can have a devastating impact on children's mental health, self-esteem, social life and school performance. In the most extreme cases, cyberbullying can even lead to suicide and self-harm.

Sometimes face-to-face bullying and cyberbullying occur alongside each other. Peer pressure can lead to cyberbullying.

Children are often afraid or embarrassed to tell others that they are being cyberbullied. This is why it's important for parents and educators to build trust with children and be aware of the signs of cyberbullying such as being upset or secretive about online activities and phone use; anxiety or distress; or changes in social behaviour like not wanting to go to school or appearing lonely.

#### What should I do if I think my child is being cyberbullied?

- Be friendly, listen to your child and talk to them calmly about what is happening.
- Monitor your child's activity, who they are interacting with, and learn to recognize the signs of cyberbullying.
- Collect evidence of the cyberbullying such as taking screenshots, so you have proof in case you need to report it to the

authorities.

- Help the child block or unfriend the people who are cyberbullying on social media and teach them not to respond to such bullying messages.
- Recognize that bullying can take place both face-to-face and online, and support your child in every aspect of society.

#### A Guide Book for Parents:

To keep Children Safe from Online risks

- Report bullying to social media channels.
- Support your child, get help from their teachers, reach out to the child protection helpline at 1121 for assistance and support services, report to PTA and FIA or register a complaint with NCRC.
- Teach your child to behave positively online, to protect themselves and others. Anything they post online or share with

others can leave behind a trail of information about them. Your child should always make sure they're leaving a good "digital footprint" and be mindful about what they do and say online.

 Make sure your child understands that no one should spread rumours or share hurtful or embarrassing jokes, stories and photos. What may seem like a harmless joke to one person can be hurtful to others.

#### Harmful content



Children mav come across inappropriate content online, such as pornography, violence, misogyny, xenophobia, inciting suicide and self-harm. This may promote and normalize negative behaviours, with harmful impacts on a child's personality, education and emotional development. Children may suffer from poor mental health, engage in sexism and objectification of women, or experience sexual violence and other negative outcomes.

#### What can I do if I think my child is accessing inappropriate content?

- Stay calm and don't be judgemental, or blame or punish the child. Ensure that your child understands you will believe them and protect them.
- Have open conversations with your child about the content they have viewed to help them process their feelings about it and develop critical skills.

parental controls on the software

your child uses, and know how to

access support services like PTA.

FIA. NCRC and the 1121 child

protection helpline.

- Talk about the importance of respecting girls, boys, women and men, and of living in a peaceful and tolerant society.
- Ensure you are familiar with

#### Fake news and misinformation

Unfortunately, a lot of fake news and false or misleading information can be found online and spread on social media. Spreading fake information and news without first verifying its source and authenticity can have severe consequences, both personally and for society as a whole. Many people, including children, find it difficult to distinguish between reliable and unreliable information, and forward it to other people without realizing the harm it causes. they understand the world, so it is important they are able to critically evaluate news and information they see online. Fake news can cause anxiety or lead to negative actions or even violence.



What children see online shapes how

## What can I do if I think my child is accessing fake news and misinformation?

- Teach your child to think critically about the news and information they see online and to always corroborate it from reliable sources before passing it on.
- Teach your child to be especially critical about information and news they receive on social media, such as through WhatsApp forwards, Facebook, TikTok and YouTube.



PTA EXPLAINS: What is fake news? https://www.youtube.com/watch?v=0n-5oLHfD54

#### **Excessive online activity**

Too much time in front of a screen isn't good for anyone's physical, emotional or mental health. It's important for your child to maintain a healthy balance between online and offline activities.

While online gaming need not be harmful in itself, too much gaming

can have physical and psychological consequences. Children who get addicted to online gaming may start neglecting school and their personal well-being, become more aggressive, isolated from friends and family, or experience mental distress or health issues. Some games also have financial costs.

#### What can I do if I think my child is spending too much time online?

- Be a positive example and reduce your own screen time – whether on your phone, computer or television. Propose shared activities you can do with your child and other family members and friends that take all of you away from the screen and spend time together: walking, cooking, playing boardgames, telling stories, playing charades, painting, etc. – anything that is healthy and makes the child happy.
- Together with your child, agree on how much screen time is appropriate and how to balance it with other activities.
- Use parental controls to limit your child's screen time.
- Empower them to make good decisions and empower them not to give in to peer pressure.
- Be aware of which online games your child is playing, take an interest in them, and maybe even join in sometimes!

#### Cybersecurity risks

Clicking on the wrong links, opening strange attachments, or downloading anything from unsafe sources can cause serious problems for children and adults. It can put a software on their gadgets that can spy on them, steal their personal information, or send spyware or harmful viruses to other people online. It's important that children are careful about what they click and download!

You and your child should always be aware of the importance of maintaining online privacy. This includes keeping personal information private, not sharing their passwords with others, or allowing others to log into their accounts.



#### What can I do if I think my child is facing cybersecurity risks?

- Teach your child to never give out private information online or share their passwords with others.
- Teach your child never to open a strange attachment, even from someone they know, or click on a strange link, such as those with spelling mistakes, strange numbers or symbols.
- Teach them to always think first before opening texts, messages and emails from someone they don't know.
- Teach your child to be suspicious of unexpected or unusual messages even if they seem to come from someone they know, or from a government institution,

the police or a bank. Always think about why the sender is requesting such information, and try to double-check it by contacting the sender through some other means.

- Teach them to be especially careful when they are offered something for free or at an oddly low price – it might be a scam.
- Report the suspicious link to the social media company or digital platform and to PTA.
- Change all the passwords on your and your child's accounts to strong passwords with a mix of numbers, symbols and upper and lower-case letters.

# V. HOW CAN SOFTWARE HELP KEEP YOUR CHILD SAFE?



Some parental control software is free while others must be purchased. Many social media apps and internet service providers offer free tools that you can use to keep your child safe, by:



Find a list of free and paid parental control software at the PTA website: http://www.pta.gov.pk

- stopping them from accessing inappropriate websites and content
- setting up age-appropriate content
- monitoring your child's app usage and purchases
- keeping track of your child's location
- deciding how much time your

child can spend on the device or on certain apps

- limiting exposure to adult content and blocking pornography
- managing which devices are used and what they can access on your home internet connection
- restricting search results for children so they don't find inappropriate content

#### **REMEMBER:**

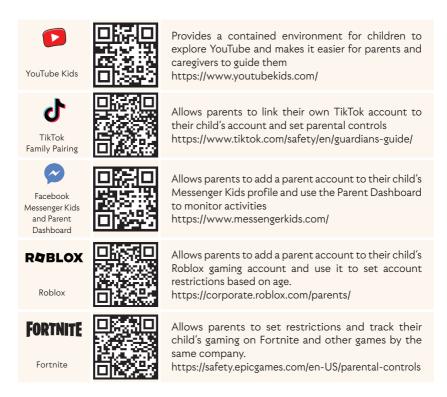
Parental control tools provide a technical solution to directly control children's online activities. But these tools become ineffective as children mature and gain independence. This is why it's crucial to impart and cultivate the skills your child needs to think critically and practice self-control.

#### Using built-in parental controls in online apps

Many apps come with their own sets of parental controls.

You can set these controls so they automatically place restrictions based on your child's age. You can also customize them and monitor your child's engagement with the platform.

It's a good idea to check the app's default settings and then adjust them if you need. When setting up accounts, make sure your child gives their correct age so they get the right content for their age group. In fact, many apps don't allow children to sign up if they are below a certain age, so you can make sure your child only uses apps and games that are suitable for them. Here are a few examples of popular apps used by children and their parental control settings. You can find more information on the PTA website (http://www.pta.gov.pk).



#### **REMEMBER:**

Have open conversations with your child about parental control settings and why they're needed.

This will help you create a healthy and balanced online experience for your child, build trust between parent and child, and respect their privacy, autonomy and educational needs.

#### Using parental controls offered by internet providers

Many internet service providers (ISPs), from whom you purchase internet access, have tools to help you keep your children safe online. These can block harmful websites and content and establish secure connections that can help reduce cybersecurity risks.

#### Using safe browsing options in search engines

You can use search engines like Google and Bing to restrict searches and prevent children from finding inappropriate or harmful images, videos and text.

On both Bing and Google, you can activate SafeSearch and set it to strict

filtering. On Google, you can also use Family Link which gives you more advanced parental control measures.

While these safety settings are good at filtering online content, they are not perfect. Sometimes, harmful content might still slip through.





Enables parents to limit screen time, filter content and understand how their child spends time online. <u>https://safety.google/intl/en\_uk/families/</u>

#### **REMEMBER:**

Safe browsing settings only work on the search engine where they have been set up. If only Google SafeSearch is activated, it will still be possible to find harmful content using Bing. To be safe, remember to activate safe browsing on all search engines.

### **KEEPING CHILDREN SAFE ONLINE**

The digital revolution has made it possible for even the most marginalized children to learn, communicate and make their voices heard. But as children spend more time online, it brings new risks.

Parents and caregivers can help to safeguard children against these online hazards.

#### Be aware of online risks

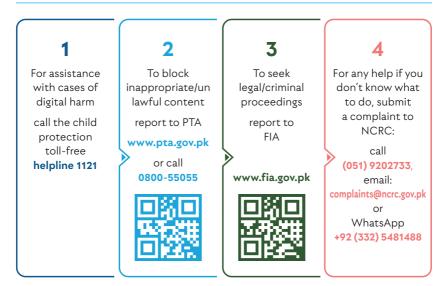
- Child online sexual exploitation and abuse
- Cyberbullying
- Harmful content

#### Safeguard children online

- Be a good online role model for your child
- 2. Build trust and communicate openly
- 3. Don't blame your child for their negative online experiences
- Teach your child how to recognize and respond to inappropriate online behaviour
- 5. Set clear ground rules for internet use

- Fake news and misinformation
- Excessive online activity
- Cybersecurity risks
- 6. Encourage your child to think critically
- Encourage a healthy balance between online and offline activity
- Use available tech tools and reporting lines to keep your children safe
- 9. Empower your child to stand up to peer pressure

#### Get help against online risks



### GLOSSARY

Age-appropriate content	Images, text and videos that are unsuitable for a child depending on their age. For example, violent, emotionally intense or sexually explicit content may be inappropriate for young children.
Attachment	A document, image or file that is included with an email or message. You should avoid opening attachments sent by people or accounts you don't know.
Blocking	Blocking is a way of keeping unwanted people away from you online. When you block someone on a service, they can't talk to you or see the things you share on that service.
Child	Any human being below the age of 18 years. Pakistan ratified the Convention on the Rights of the Child in 1990, and is committed to uphold the rights of all children to protection, both online and offline.
Hacker	A person who breaks into someone else's account or computer system, often for bad purposes like stealing information or doing illegal activities.
Internet service provider	The company that provides your internet connection, such as PTCL.
Messaging service	Apps and websites that give a way to send messages, videos, images and voice notes. Popular services include WhatsApp, Facebook Messenger, Signal and Telegram.
Online gaming	Video games that are played online, often with many other players. Online games often have chats and other ways for players to communicate in the game.
Parental control software	Software with settings that help parents restrict and monitor how their child uses the internet.
Personal information	Personal information is all the information that relates to you. It includes your name, age, phone number and email, usernames and passwords for accounts, your home address or your school. It can also include your personal interests, political views or religion.
Scam	A scam is a way of tricking people into handing over money, images or personal details, or doing something that they don't want to do. Scammers can often seem friendly or pretend to be people you know.
Search engine	A website or app used to find information on the internet. Popular search engines include Google, DuckDuckGo and Bing.
Social media	Apps and websites that people use to share information, images and videos with each other. Popular social media platforms include Facebook, TikTok, Instagram and Twitter (X).
Spam	Unwanted messages, emails, text messages or calls you receive, usually from people you don't know. It's important to be careful with spam and not click on suspicious links or share personal information.



#### **Technical Contributions by:**

United Nations Children's Fund (UNICEF) Pakistan and HQ, Telenor Pakistan, National Commission on the Rights of the Child, February 2024