Parent's Guide On

Online Safety

Table Of Contents

Tips For Parents On

Online Safety

The internet is vast, so connect with your child by casually discussing the apps you both use, including games. This can help open up conversations.

To understand their digital world and build trust,

Explore Together

Sit down together and explore the web and mobile applications that your child is interested in using, including games.

To ensure personal information is protected,

Explore Privacy Settings

Explore settings that can be applied to your child's devices and applications used for school, communication, or leisure purposes.

To protect your child's online presence and data,

Enforce Privacy Settings

Review the permissions for all the apps on the device used by your child.

To empower your child to recognize and avoid online threats,

Educate On Online Risks

Talk about potential online dangers and discuss topics like cyberbullying, phishing, trolling and inappropriate content.

To promote healthy habits,

Set Screen Time Limits

Set and enforce screen time rules to help your child understand their importance and balance online and offline activities.

Family Media Plan

Guidelines

1 Designate ‘No Device’ Zones

Establish areas in the house where devices are not permitted, such as dining rooms and bedrooms.

2 Monitor And Limit Screen Time

Set daily limits to ensure a balanced lifestyle with time for exercise, reading, and family interaction.

3 Use Parental Controls

Use tools to manage and monitor your child’s online activity to ensure they access age-appropriate content.

4 Educative & Creative Screen Use

Encourage using digital devices for learning and creativity instead of just watching videos or scrolling through social media.

5 Lead By Example

Model good device habits by following the same rules you set for your children.

Is My Child Ready For Social Media?

Discuss The Goal

Understand their intentions:

- Discuss your child’s interest in social media and recommend other ways to stay engaged.

Familiarise yourself:

- Learn about all the platforms your child is interested in.

Start Together

Set up together:

- When you decide it’s okay for your child to join social media, create the account together.

Share Credentials:

- Require that they share their login details with you.
- Ensure you follow them on the platform.

Online Safety Tips

Friend requests:

- They should not accept requests from people they do not know.

Offensive behaviour:

- They should unfriend/block somebody doing something offensive on social media.

Taking Breaks

Recognise toxicity:

- Encourage your child to take a break from social media when it feels toxic.

Self-reflection:

- Taking breaks can help them understand why they use social media and how it affects their feelings.

Monitor

Filter awareness:

- Regularly check your child’s social media and encourage them to follow accounts that promote body positivity and healthy self-image.

Bonus Tip:
Children should only join social media once they reach the age recommended by the platform.

Regular Digital Media Discussions

Regular Check-Ins

Evening conversations

Ask everyone what was the most inspiring or frustrating thing they saw online that day to encourage sharing and reflection on digital experiences.

Post-School Inquiry

Talks after school

Ask your children about tech tools they used in school and their opinions on them to promote awareness of educational technology and its impact.

Weekly App Review

End of week activity

Ask everyone to track the applications they spent the most time on and brainstorm ideas for more balanced usage to help manage screen time and promote healthier digital habits.

Digital Literacy

Introduce Family learning time

Discuss topics like online privacy, cyberbullying, artificial intelligence and online presence regularly to educate one another on safe and responsible internet use.

Explore New Technologies

Joint exploration

Discover and learn about new apps, games or technologies as a family to keep the family up-to-date and engaged with new digital trends.

Bonus Tip:
This includes websites, game apps and social media platforms.

What Does Cyberbullying Look Like?

1. **Sending Threatening or Harmful Messages**
   Cyberbullies send harmful, threatening, or insulting messages to cause fear, anxiety and distress to the recipient.

2. **Spreading False Rumours Online**
   Cyberbullies spread false information or rumors about someone online damaging reputations and relationships, and causing emotional pain.

3. **Posting Hurtful Or Embarrassing Content**
   Cyberbullies post photos, videos, or comments intended to hurt or embarrass someone, leading to humiliation and loss of self-esteem for the victim.

4. **Impersonating Someone To Ruin Their Reputation**
   Cyberbullies create fake accounts or impersonate someone to cause harm to their reputation, resulting in mistrust, confusion, and damage to the victim's social standing.

5. **Excluding Someone From An Online Group Intentionally**
   Cyberbullies intentionally leave someone out of online groups, chats or activities causing feelings of isolation and loneliness for the excluded person.

Call To Action on Cyberbullying

Build Trust With Your Child

Actively listen with empathy and cultivate a comfortable environment for ongoing dialogue about their digital world.

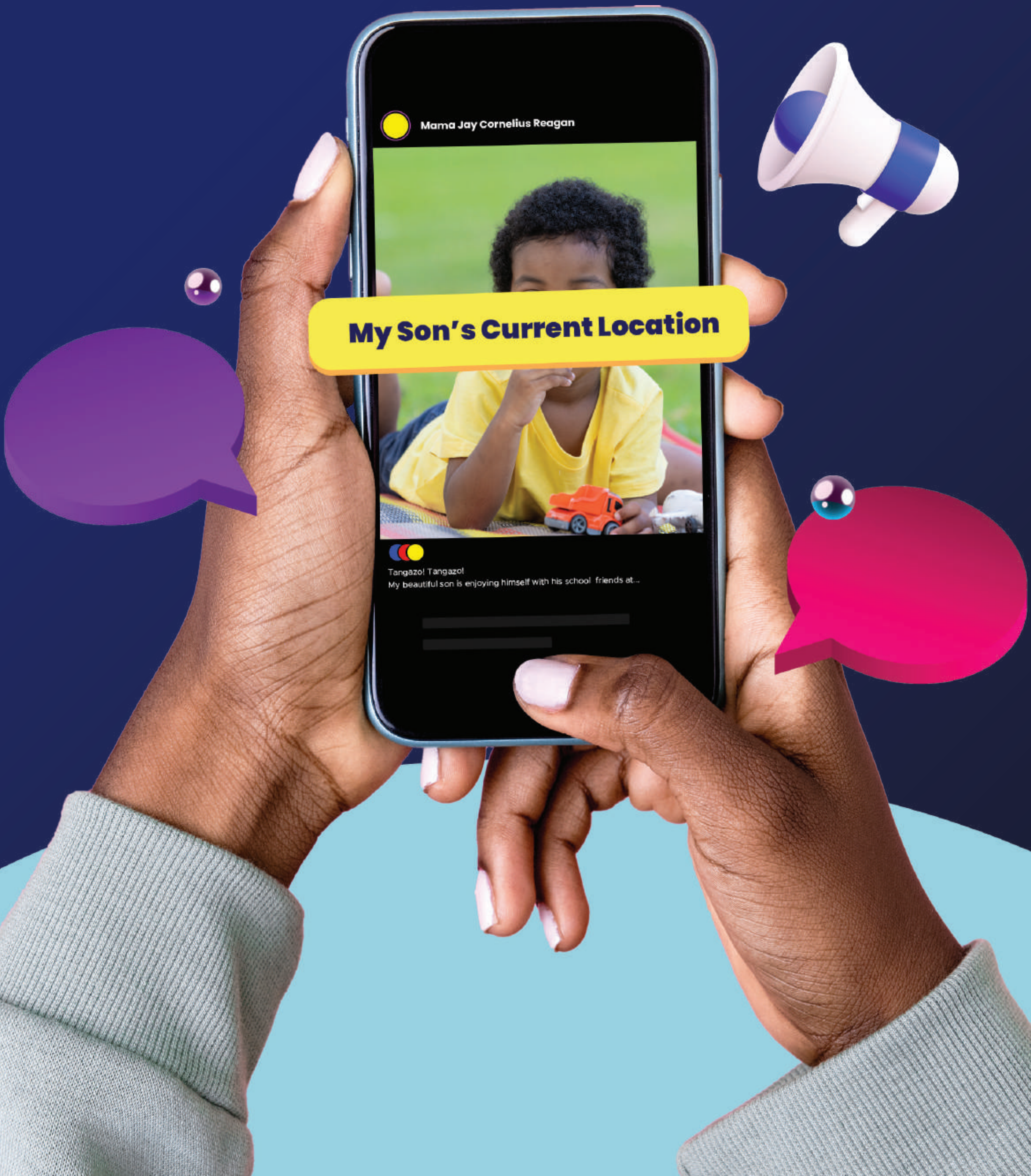
Create A Safe Space

Stay calm when discussing your child's online activities, ask questions to understand better, and offer guidance in a way that encourages open communication.

Educate

Teach your child about privacy settings and the importance of keeping personal information secure while discussing the potential risks and benefits of social media.

Oversharing



Mama Jay Cornelius Reagan

Tangazo! Tangazo!
My beautiful son is enjoying himself with his school friends at...

Location Overshare

Be Mindful:

- Avoid sharing posts that reveal you and your child's location.
- This includes photos from school events, extracurricular activities, or your neighborhood.

For Example:

- Sharing school trip photos with your child's last name visible can reveal their location and put them at risk by giving strangers access to this information

Mind Your Child's Digital Footprint

Long-Term Impact:

- The internet has a long memory; today's post can affect your child's future.

For Example:

- Sharing funny pictures or stories might embarrass your child later, as employers or school admissions officers could see them and consider them unprofessional affecting their opportunities.

Building Healthy Online Habits

Open Dialogue:

- Talk openly with your child about online safety and appropriate sharing.

Privacy Settings:

- Teach your child about privacy settings on social media platforms. Review the permissions for all the apps on your phone.

For Example:

- Navigate to Settings >> Location >> App Permissions to see which apps have access to your location and adjust as needed.

Selective Sharing:

- Encourage your child to be selective about what they post and who they share it with.

Family Guidelines:

- Create family guidelines for online behavior, focusing on responsible sharing and safe internet practices.

Trolling

Trolling is when someone intentionally posts irrelevant, or offensive messages online to upset others and disrupt conversations.

These messages can appear on social media, forums, and comment sections of websites.

How Does It Impact A Child?

- Emotional distress.
- Damaging their online reputation.
- Creating anxiety that discourages online participation.
- Makes them feel unsafe online, hindering their ability to connect and learn.

How Can You Protect Your Child?

- Discuss openly what it looks like, how it can make them feel and the importance of respectful online communication.
- Empower your child to recognize trolling behavior and encourage them to ignore.
- Discuss the importance of reporting inappropriate behavior.
- Work together to navigate the online world safely and responsibly.

Phishing Scams

Phishing is a scam where attackers pretend to be a trusted person or company to trick you into giving personal information, often through fake emails, messages, phone calls or websites that look real.

Spot The Phish

Identify Red Flags:

- Urgent Language: Watch for emails, text messages or phone calls pressuring immediate action.
- Requests for Personal Information: Exercise extreme caution with people, phone calls, messages or emails requesting for passwords, ID numbers or bank details.

Talk to Your Child

Educate About Phishing:

- Frequently talk about the dangers of phishing with the whole family.
- Give examples of phishing scams scenarios that may be through phone calls, emails and messages to help them recognize suspicious messages.

Stay Vigilant

Be Proactive:

- Use Strong Passwords and Multi-Factor Authentication (MFA) on accounts.
- Keep Software Updated: Including operating systems and security softwares.
- Question Unsolicited Offers: Be skeptical of messages offering deals that seem too good to be true.

A Parent's Guide to

Password Management

Strong passwords are your family's first line of defense in the digital world. Here are three key points to remember:

Build A Strong Password

Length Is Strength:

- Aim for passwords at least 8-12 characters long.

Mix It Up:

- Use a combination of uppercase and lowercase letters, numbers, and symbols (@, #, $) to create complexity.

Be Unpredictable:

- Avoid using personal details like birthdays or names
- Treat each account like a separate lock with its own strong, unique password.

Remember Responsibly

Options for Remembering:

1. Password Managers:

- These are secure apps that store passwords with a master password. They can generate and remember strong passwords for you.

2. Create A System:

- Develop a base password and customize it for each account.

3. Mnemonic Devices:

- Use a memorable phrase with letters, numbers, and symbols.

Bonus Tip:

Talk to your child about password safety and why strong passwords are crucial. Remind them never to share their password with anyone.

A Parent's Guide to

Mobile Money Safety

Mobile money is a convenient way to manage finances, but it's also a target for fraudsters. Here are three key points to keep your family safe:

Guard Your PIN Like Gold

Create A Strong PIN:

- Choose a unique combination of numbers that's difficult to guess.

Keep It Secret, Keep It Safe:

- Never share your PIN with anyone, including family or friends.
- Avoid writing down or storing it on your phone.

Change Your PIN Often:

- This will protect you from any leak of your pin.

Always Double Check

Verify Every Transaction:

- Always confirm recipient details (phone number, name) before sending money.

Stay Vigilant:

- Scammers create urgency to pressure you into hasty decisions.
- Take time to verify requests before sending money.

Monitor Your Account:

- Regularly review transaction history for unfamiliar activity.

Fight Fraud

Review Suspicious Activity:

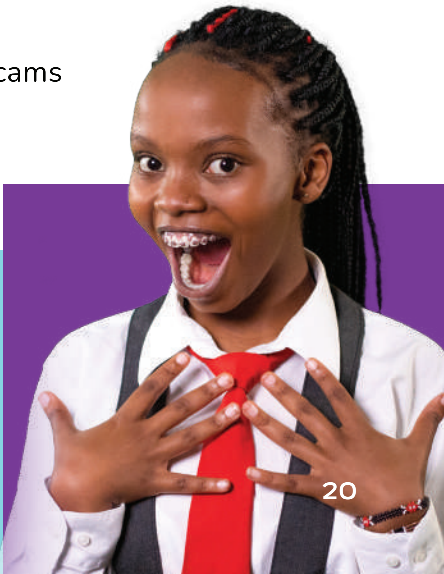
- Immediately report suspicious messages or unusual account activity to your bank or mobile money provider.

Stay Informed:

- Keep yourself updated on common mobile money scams to stay vigilant.

Bonus Tip:

Avoid public networks and use secure, private networks for mobile money bank transactions to prevent fraud.



FLASH SQUAD