Child Online Protection

ITU Global Programme

Guidelines for parents and educators on Child Online Protection 2020

Karl Hopwood

Online safety expert - Insafe

> *"It is essential to discuss openly the risks that exist for children and young people online, to teach them how to recognise risk, and prevent or deal with harms should they materialise without unduly frightening or exaggerating the dangers."*

Guidelines for parents and educators on
Child Online Protection
2020

2009

iPhone 3GS

ANNOUNCED:
June 8, 2009

RELEASED:
June 19, 2009

KEY FEATURES:
Twice as fast as the previous version, and less expensive.

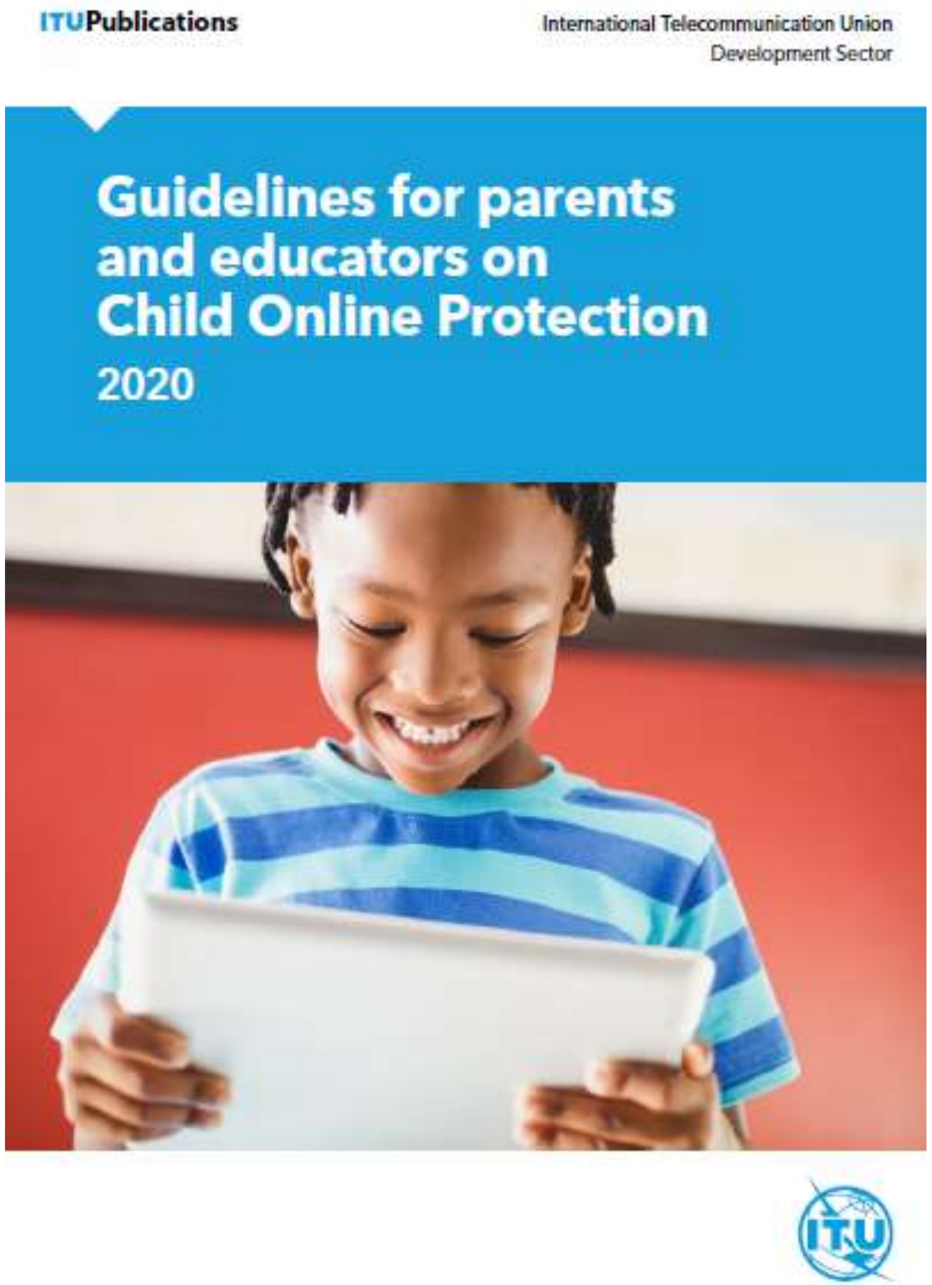
PRICING:
8GB model, $99;
16GB version, $199;
32GB model, $299

Minecraft

Child Online Protection

The aim

To raise awareness of the scope of the challenge and provide a resource that will help [parents, carers and educators] to effectively support young people’s interaction with the online world



ITUPublications

International Telecommunication Union
Development Sector

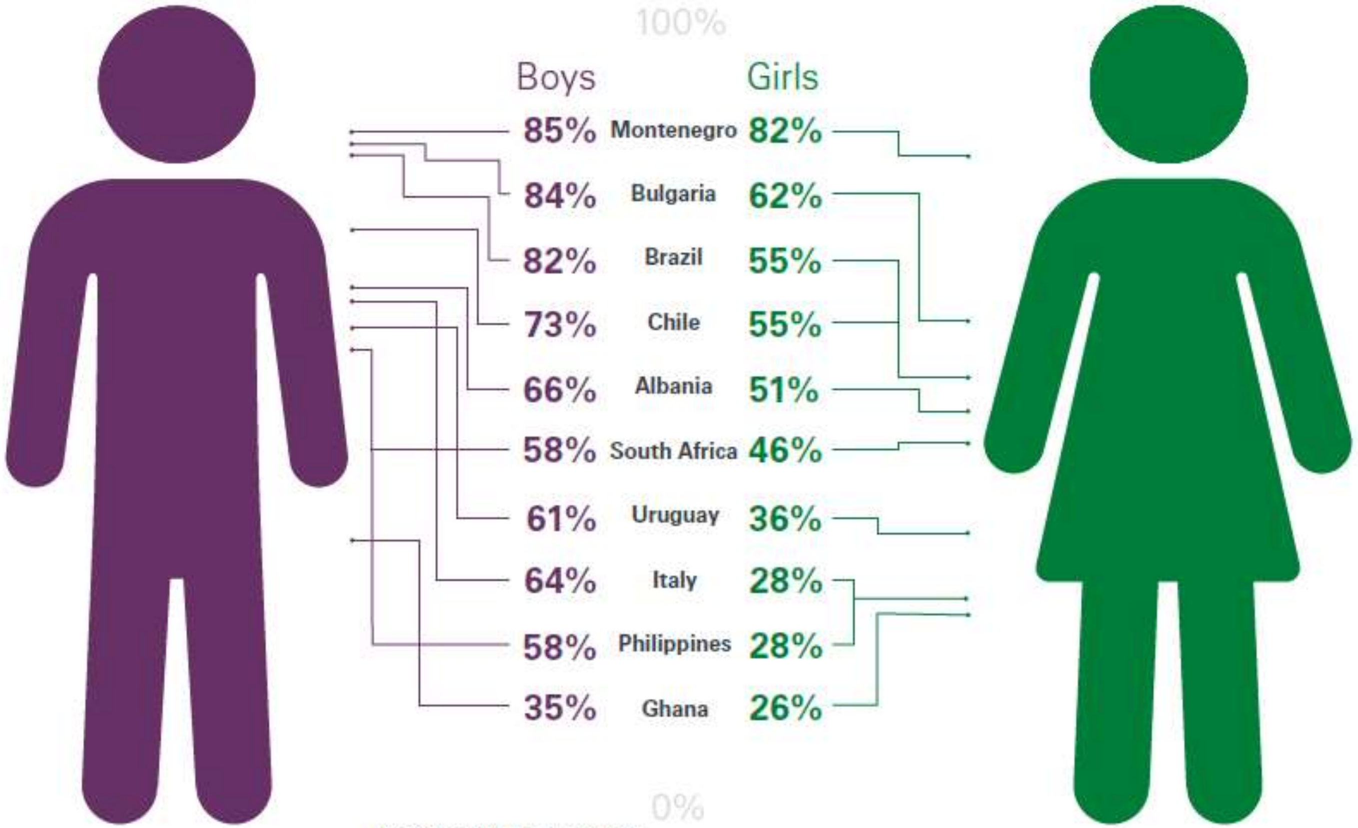
Guidelines for parents and educators on Child Online Protection

2020

Child Online Protection

Children and young people in a connected world

Figure 2. Children who play games online at least weekly, by gender



Base: Children aged 9-17 who use the internet

Children with vulnerabilities

Some children and young people with disabilities may face difficulties in using, or even exclusion from online environments due to inaccessible design…or the need for appropriate support.

Some parents of children and young people with disabilities may be overprotective because of their lack of knowledge on how to best guide their child's use of the internet or protect them from bullying or harassment

New and emerging risks and challenges

1. **Internet of things**
2. **Connected toys and robotics**
3. **Online gaming**
4. **Voice activated technology**

Child Online Protection

Understanding risk and harms

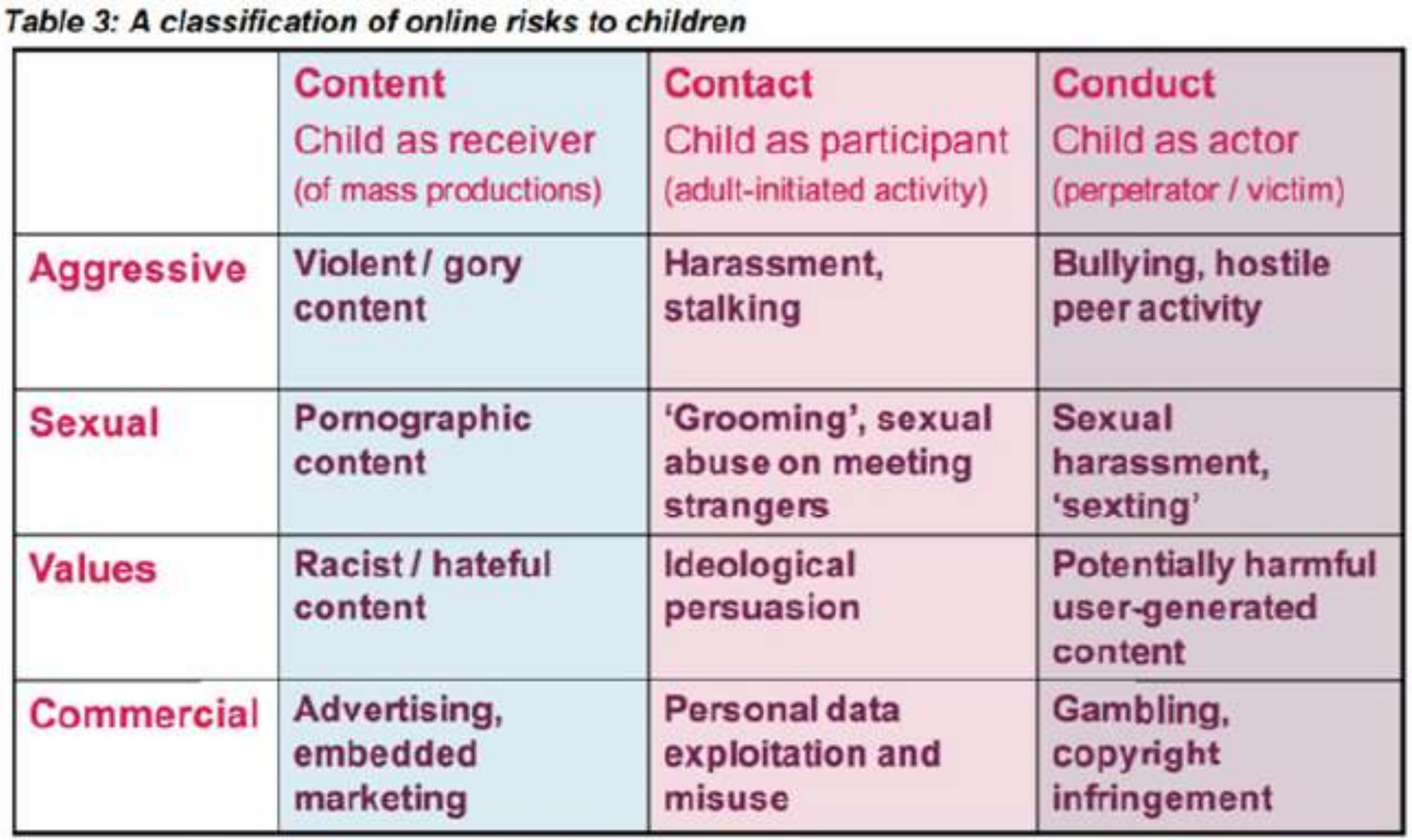


Table 3: A classification of online risks to children

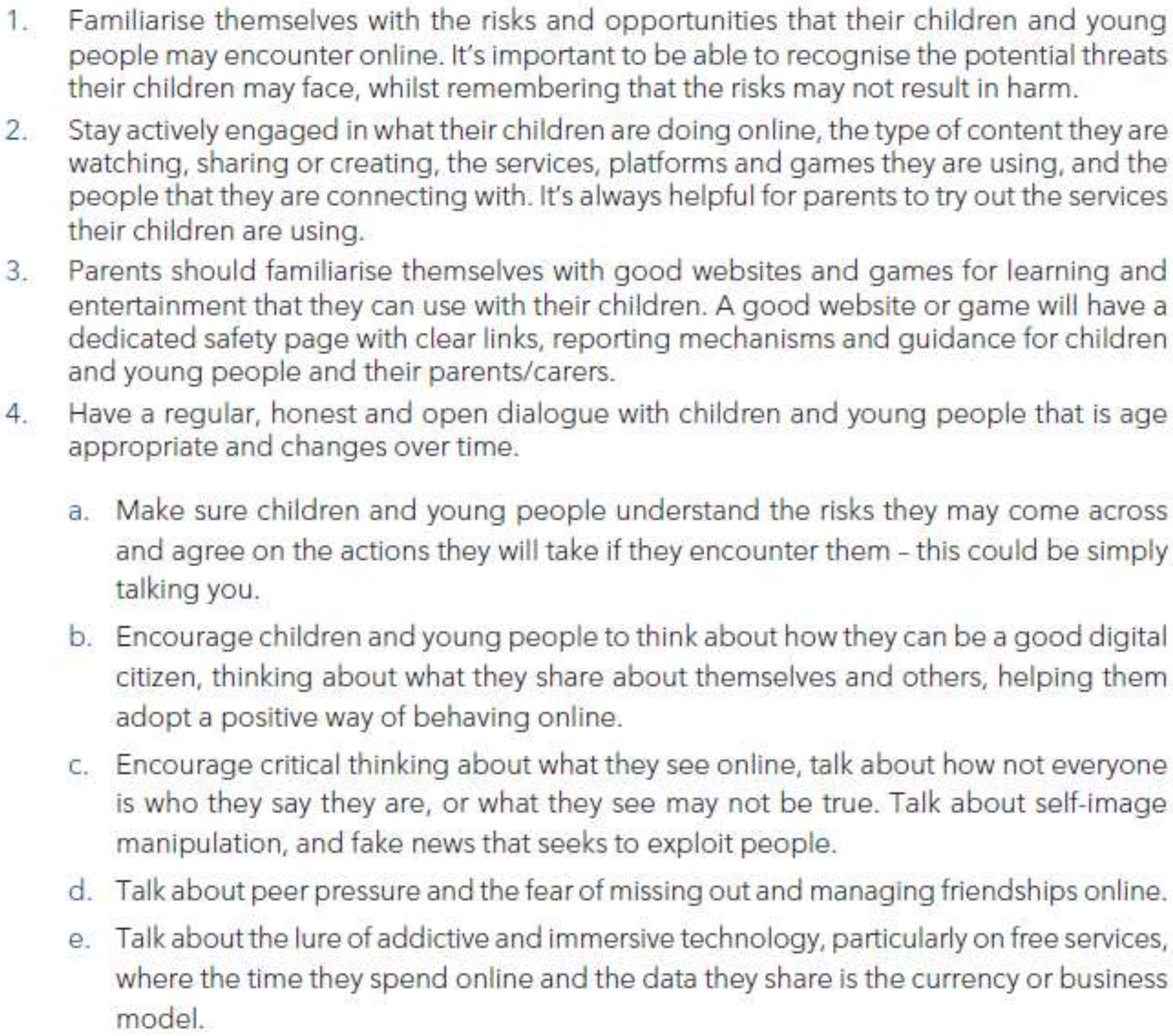
	Content Child as receiver (of mass productions)	Contact Child as participant (adult-initiated activity)	Conduct Child as actor (perpetrator / victim)
Aggressive	Violent / gory content	Harassment, stalking	Bullying, hostile peer activity
Sexual	Pornographic content	'Grooming', sexual abuse on meeting strangers	Sexual harassment, 'sexting'
Values	Racist / hateful content	Ideological persuasion	Potentially harmful user-generated content
Commercial	Advertising, embedded marketing	Personal data exploitation and misuse	Gambling, copyright infringement

Source: EU Kids Online (Livingstone, Haddon, Görzig, and Ólafsson (2011)

Child Online Protection

The role of parents, carers and guardians

1. **Importance of discussion and dialogue**
2. **Don’t overreact**
3. **Encourage critical thinking**
4. **Agree rules and boundaries**
5. **Set the right example**



1. Familiarise themselves with the risks and opportunities that their children and young people may encounter online. It’s important to be able to recognise the potential threats their children may face, whilst remembering that the risks may not result in harm.
2. Stay actively engaged in what their children are doing online, the type of content they are watching, sharing or creating, the services, platforms and games they are using, and the people that they are connecting with. It’s always helpful for parents to try out the services their children are using.
3. Parents should familiarise themselves with good websites and games for learning and entertainment that they can use with their children. A good website or game will have a dedicated safety page with clear links, reporting mechanisms and guidance for children and young people and their parents/carers.
4. Have a regular, honest and open dialogue with children and young people that is age appropriate and changes over time.

    a. Make sure children and young people understand the risks they may come across and agree on the actions they will take if they encounter them – this could be simply talking you.

    b. Encourage children and young people to think about how they can be a good digital citizen, thinking about what they share about themselves and others, helping them adopt a positive way of behaving online.

    c. Encourage critical thinking about what they see online, talk about how not everyone is who they say they are, or what they see may not be true. Talk about self-image manipulation, and fake news that seeks to exploit people.

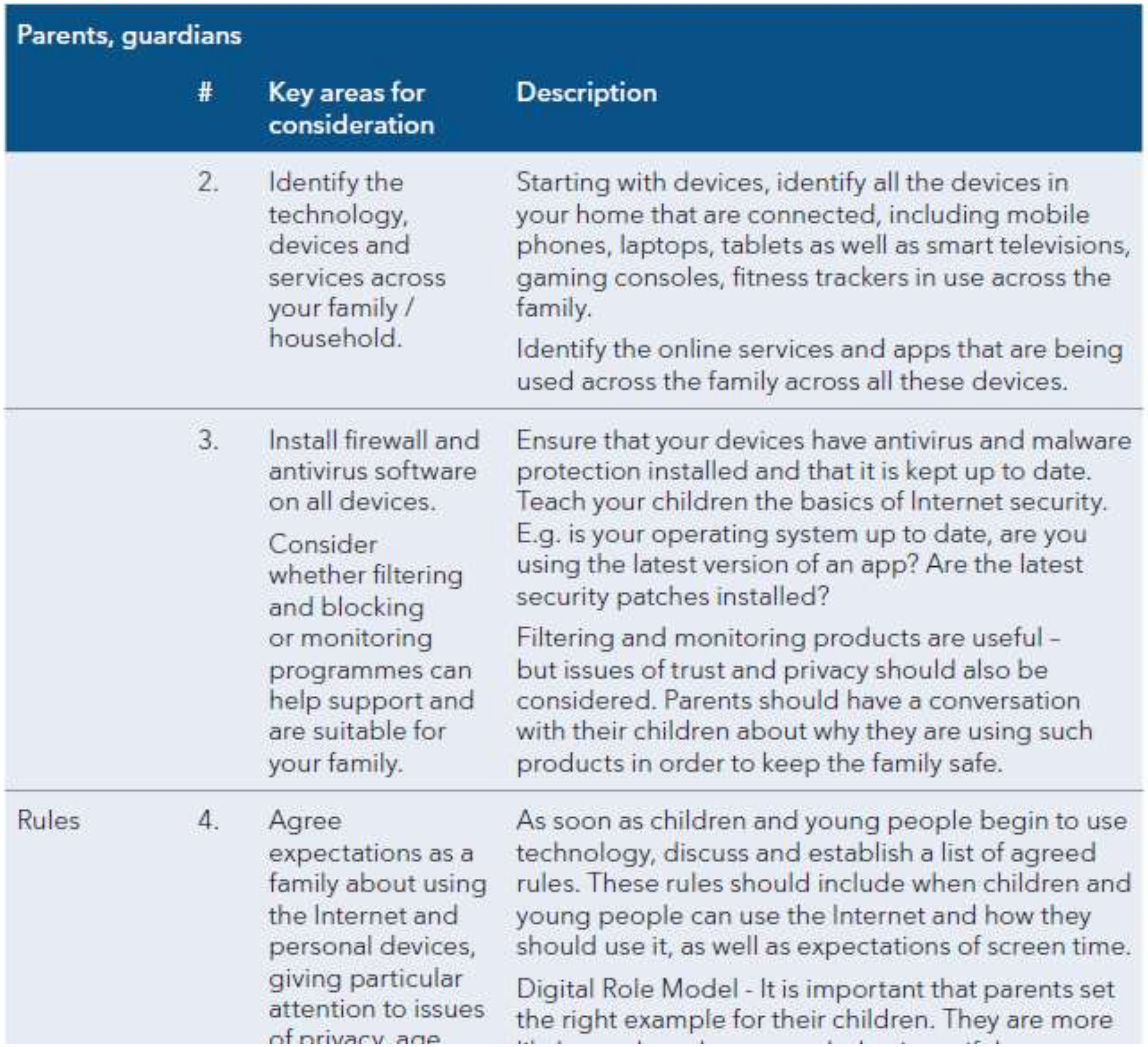
    d. Talk about peer pressure and the fear of missing out and managing friendships online.

    e. Talk about the lure of addictive and immersive technology, particularly on free services, where the time they spend online and the data they share is the currency or business model.

Child Online Protection

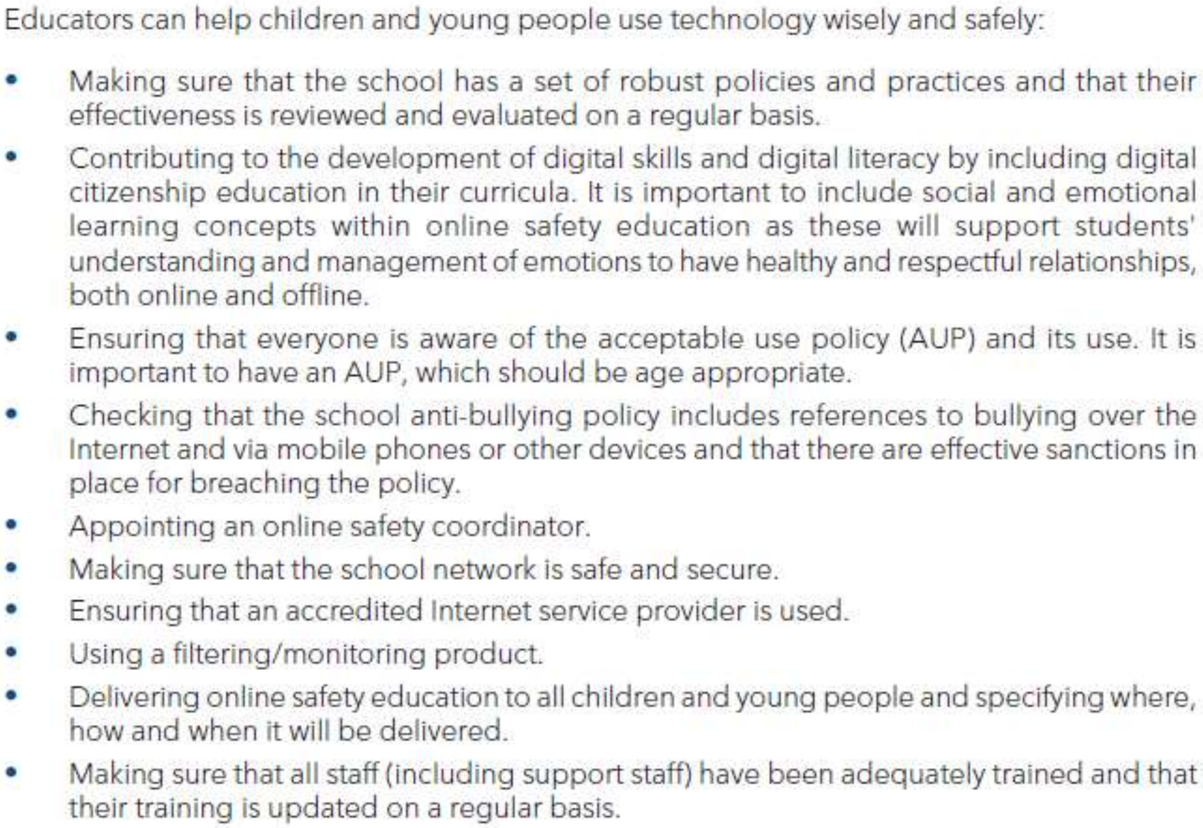
Guidelines – key areas of consideration

1. Specific suggestions
2. Practical guidance
3. Things to do



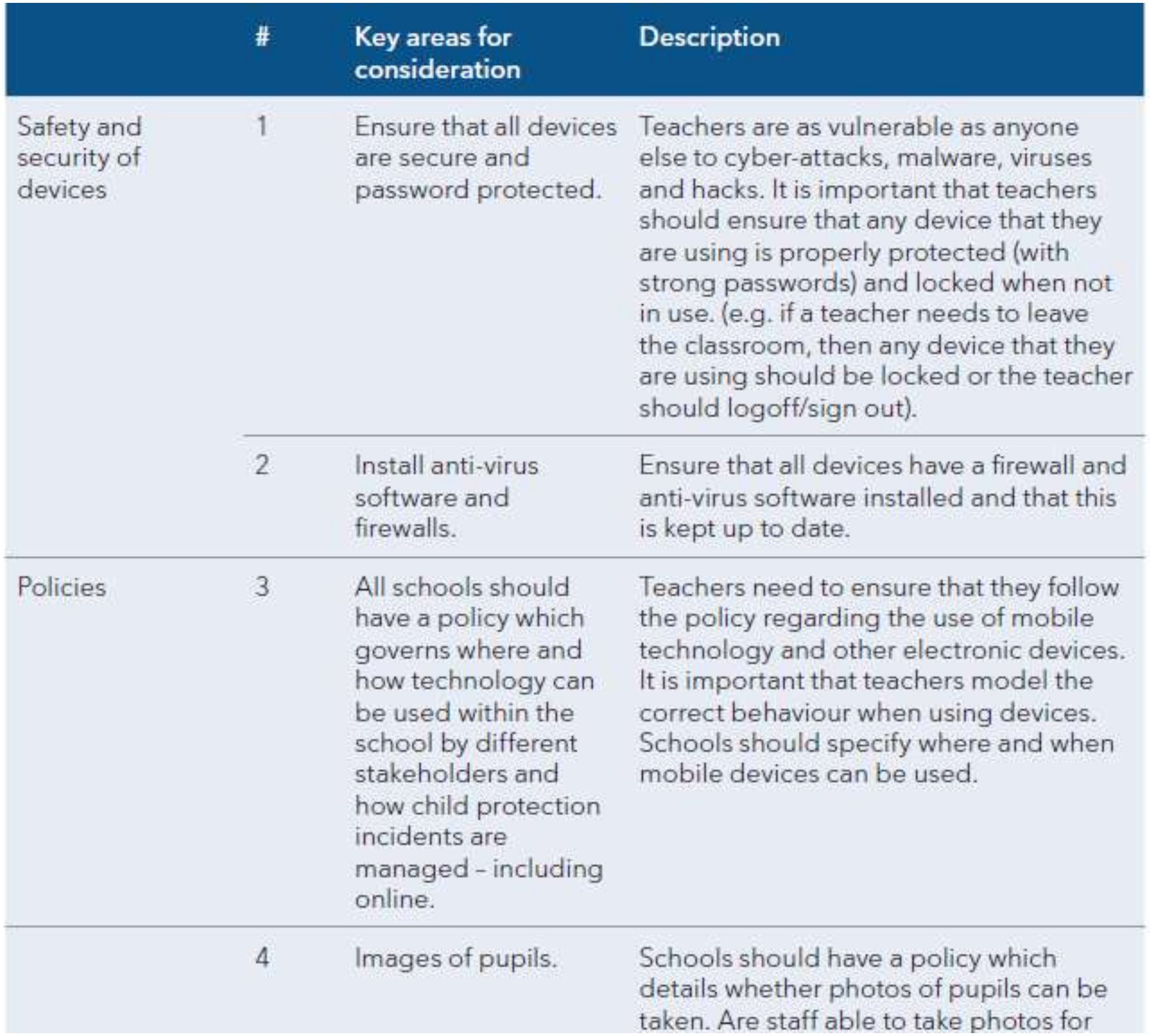
Parents, guardians			
	#	Key areas for consideration	Description
	2.	Identify the technology, devices and services across your family / household.	Starting with devices, identify all the devices in your home that are connected, including mobile phones, laptops, tablets as well as smart televisions, gaming consoles, fitness trackers in use across the family. Identify the online services and apps that are being used across the family across all these devices.
	3.	Install firewall and antivirus software on all devices. Consider whether filtering and blocking or monitoring programmes can help support and are suitable for your family.	Ensure that your devices have antivirus and malware protection installed and that it is kept up to date. Teach your children the basics of Internet security. E.g. is your operating system up to date, are you using the latest version of an app? Are the latest security patches installed? Filtering and monitoring products are useful – but issues of trust and privacy should also be considered. Parents should have a conversation with their children about why they are using such products in order to keep the family safe.
Rules	4.	Agree expectations as a family about using the Internet and personal devices, giving particular attention to issues of privacy, age	As soon as children and young people begin to use technology, discuss and establish a list of agreed rules. These rules should include when children and young people can use the Internet and how they should use it, as well as expectations of screen time. Digital Role Model - It is important that parents set the right example for their children. They are more

The role of educators / guidelines for educators



Educators can help children and young people use technology wisely and safely:

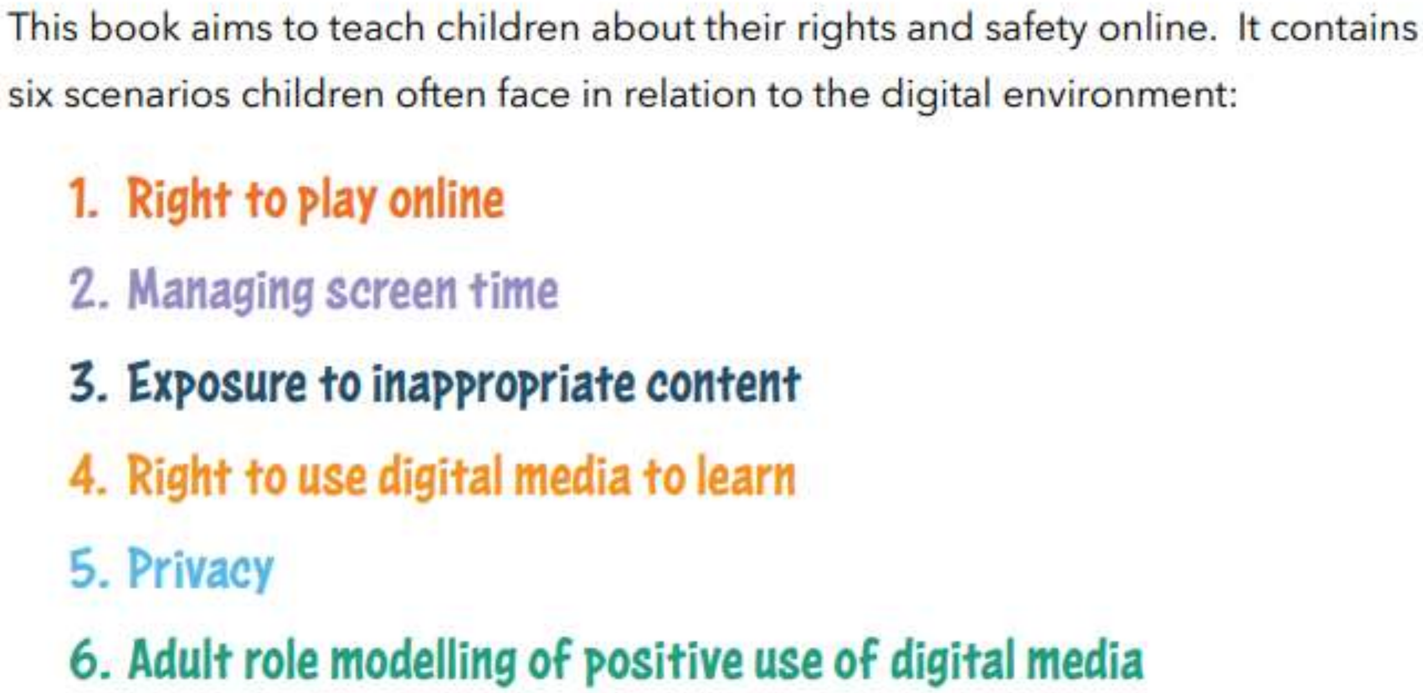
- Making sure that the school has a set of robust policies and practices and that their effectiveness is reviewed and evaluated on a regular basis.
- Contributing to the development of digital skills and digital literacy by including digital citizenship education in their curricula. It is important to include social and emotional learning concepts within online safety education as these will support students' understanding and management of emotions to have healthy and respectful relationships, both online and offline.
- Ensuring that everyone is aware of the acceptable use policy (AUP) and its use. It is important to have an AUP, which should be age appropriate.
- Checking that the school anti-bullying policy includes references to bullying over the Internet and via mobile phones or other devices and that there are effective sanctions in place for breaching the policy.
- Appointing an online safety coordinator.
- Making sure that the school network is safe and secure.
- Ensuring that an accredited Internet service provider is used.
- Using a filtering/monitoring product.
- Delivering online safety education to all children and young people and specifying where, how and when it will be delivered.
- Making sure that all staff (including support staff) have been adequately trained and that their training is updated on a regular basis.



	#	Key areas for consideration	Description
Safety and security of devices	1	Ensure that all devices are secure and password protected.	Teachers are as vulnerable as anyone else to cyber-attacks, malware, viruses and hacks. It is important that teachers should ensure that any device that they are using is properly protected (with strong passwords) and locked when not in use. (e.g. if a teacher needs to leave the classroom, then any device that they are using should be locked or the teacher should logoff/sign out).
	2	Install anti-virus software and firewalls.	Ensure that all devices have a firewall and anti-virus software installed and that this is kept up to date.
Policies	3	All schools should have a policy which governs where and how technology can be used within the school by different stakeholders and how child protection incidents are managed – including online.	Teachers need to ensure that they follow the policy regarding the use of mobile technology and other electronic devices. It is important that teachers model the correct behaviour when using devices. Schools should specify where and when mobile devices can be used.
	4	Images of pupils.	Schools should have a policy which details whether photos of pupils can be taken. Are staff able to take photos for

Child Online Protection

Storybook: under 9 year olds



This book aims to teach children about their rights and safety online. It contains six scenarios children often face in relation to the digital environment:

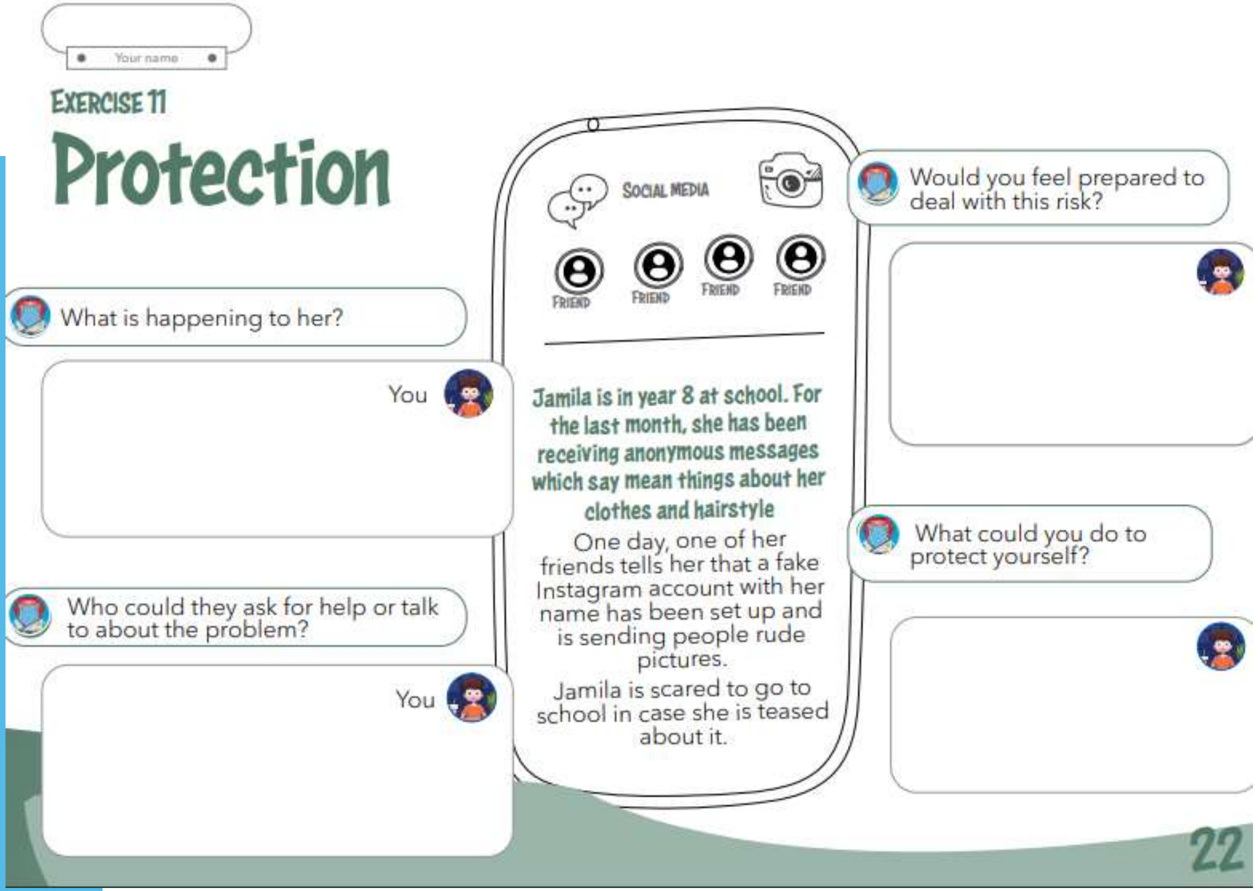
1. Right to play online
2. Managing screen time
3. Exposure to inappropriate content
4. Right to use digital media to learn
5. Privacy
6. Adult role modelling of positive use of digital media

Child Online Protection

Workbook: 9-12 year olds

Online safety activity book

WORK WITH SANGO



Your name

EXERCISE 11

Protection

What is happening to her?

You

Who could they ask for help or talk to about the problem?

You

Jamila is in year 8 at school. For the last month, she has been receiving anonymous messages which say mean things about her clothes and hairstyle

One day, one of her friends tells her that a fake Instagram account with her name has been set up and is sending people rude pictures.

Jamila is scared to go to school in case she is teased about it.

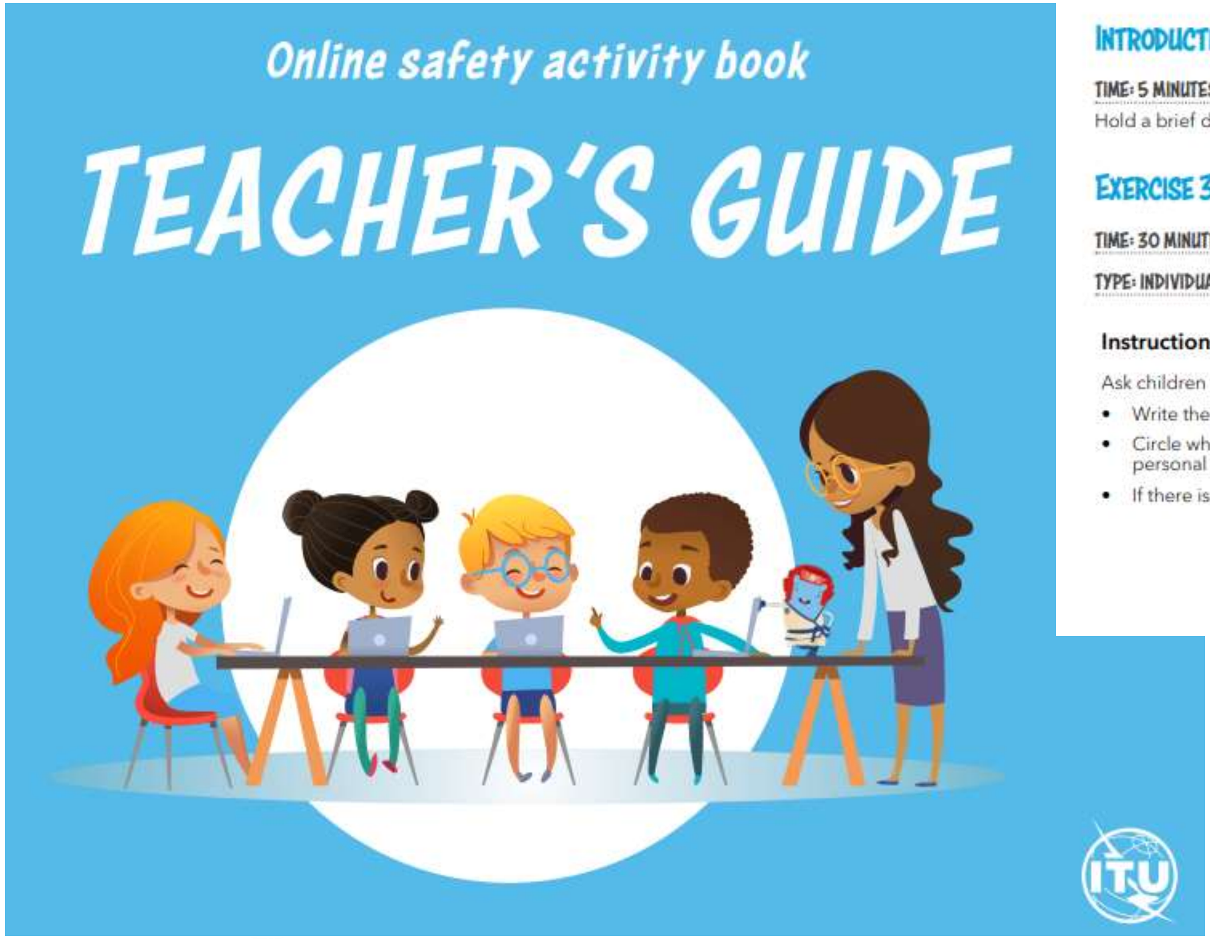
Would you feel prepared to deal with this risk?

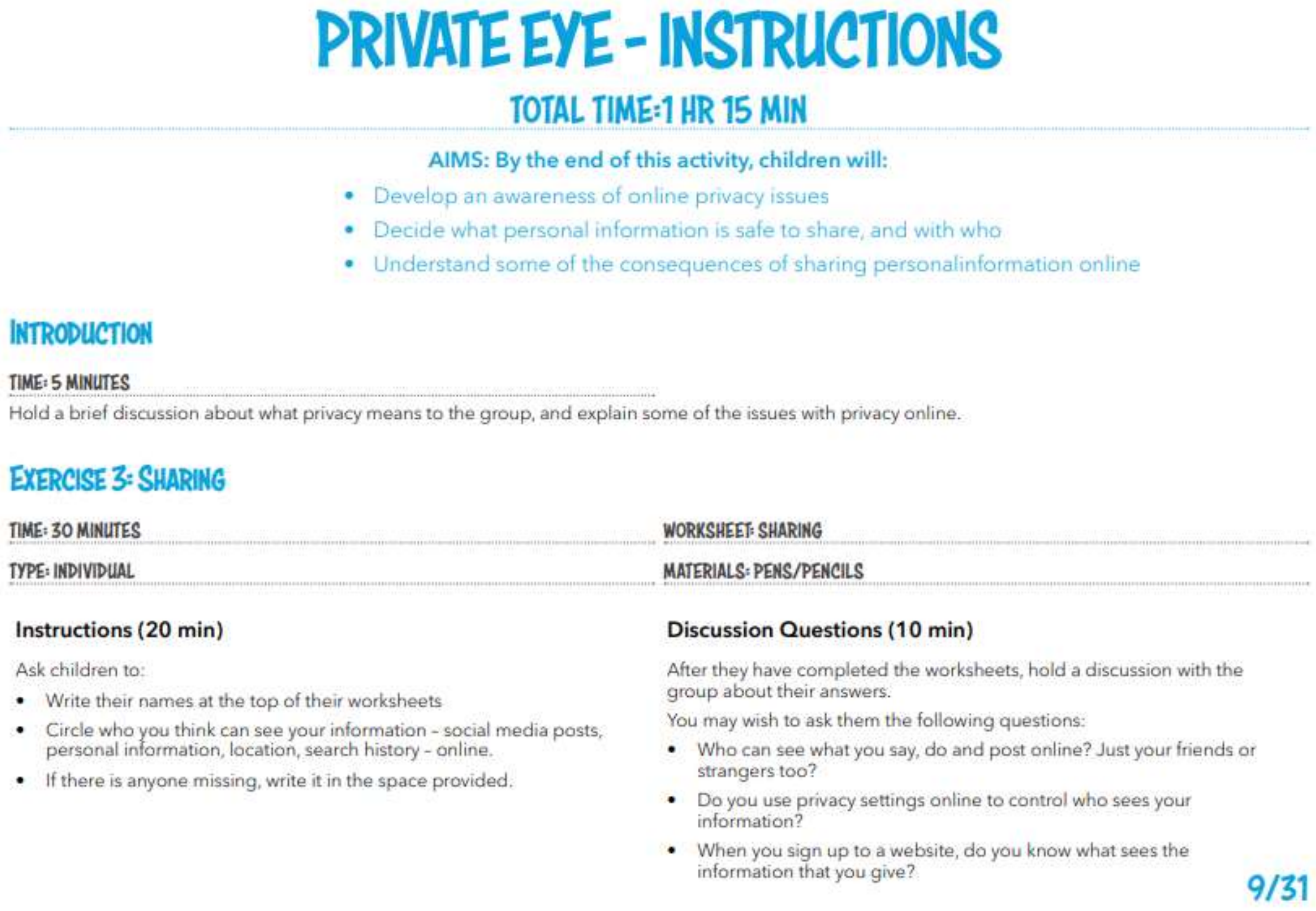
What could you do to protect yourself?

22

Child Online Protection

Teacher’s guide





PRIVATE EYE - INSTRUCTIONS

TOTAL TIME:1 HR 15 MIN

AIMS: By the end of this activity, children will:

- Develop an awareness of online privacy issues
- Decide what personal information is safe to share, and with who
- Understand some of the consequences of sharing personalinformation online

INTRODUCTION

TIME: 5 MINUTES

Hold a brief discussion about what privacy means to the group, and explain some of the issues with privacy online.

EXERCISE 3: SHARING

TIME: 30 MINUTES	WORKSHEET: SHARING
TYPE: INDIVIDUAL	MATERIALS: PENS/PENCILS

Instructions (20 min)

Ask children to:

- Write their names at the top of their worksheets
- Circle who you think can see your information – social media posts, personal information, location, search history – online.
- If there is anyone missing, write it in the space provided.

Discussion Questions (10 min)

After they have completed the worksheets, hold a discussion with the group about their answers.

You may wish to ask them the following questions:

- Who can see what you say, do and post online? Just your friends or strangers too?
- Do you use privacy settings online to control who sees your information?
- When you sign up to a website, do you know what sees the information that you give?

9/31

Child Online Protection

Social media campaign 13-18 year olds

#KNOW YOUR RIGHTS ONLINE
2

#BE PRIVATE
1

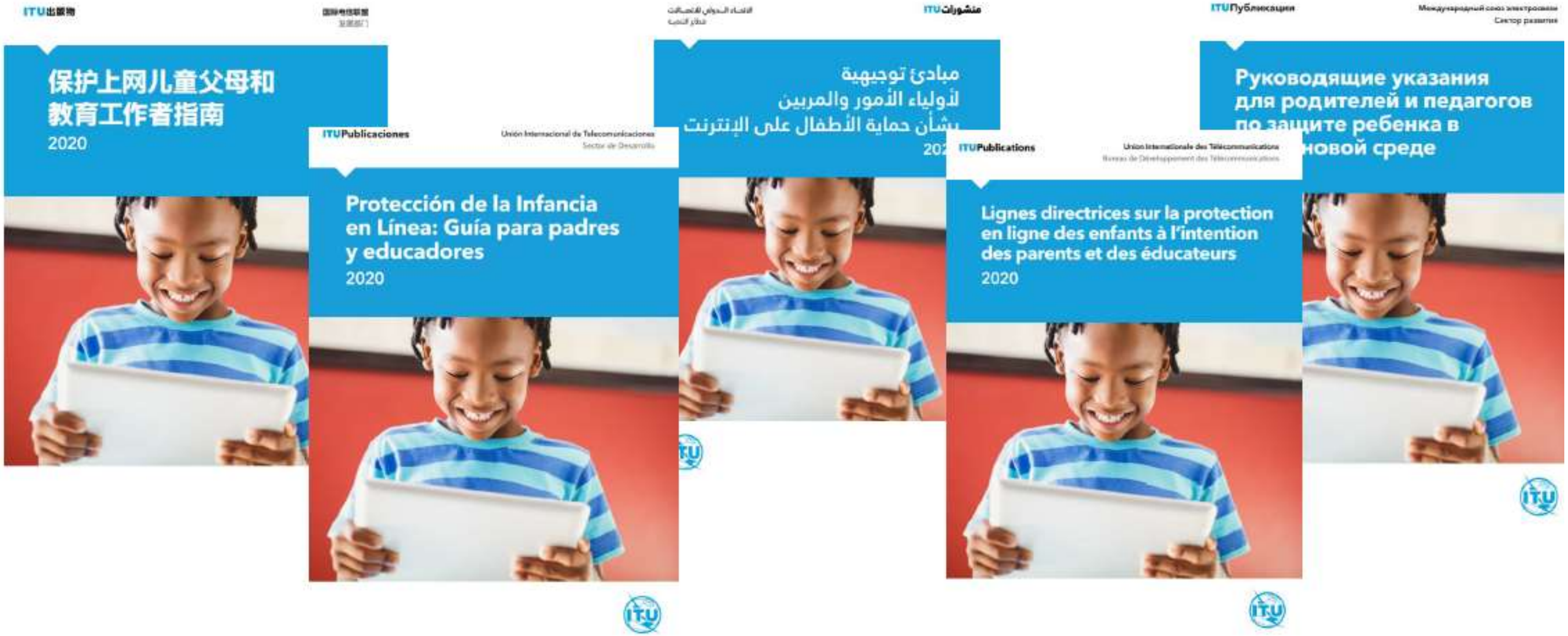
#CHECK THE FACTS

#BEWARE OF TROLLS
1

#HAVE BOUNDAIRES

Child Online Protection

6 languages – more to follow…



ITU出版物

国际电信联盟
发展部门

保护上网儿童父母和
教育工作者指南
2020

ITUPublicaciones

Unión Internacional de Telecomunicaciones
Sector de Desarrollo

Protección de la Infancia
en Línea: Guía para padres
y educadores
2020

الاتحاد الدولي للاتصالات
قطاع التنمية

ITUمنشورات

مبادئ توجيهية
لأولياء الأمور والمربين
بشأن حماية الأطفال على الإنترنت
202

ITUPublications

Union Internationale des Télécommunications
Bureau de Développement des Télécommunications

Lignes directrices sur la protection
en ligne des enfants à l'intention
des parents et des éducateurs
2020

ITUПубликации

Международный союз электросвязи
Сектор развития

Руководящие указания
для родителей и педагогов
по защите ребенка в
новой среде

Together we will protect and empower children

www.itu.int/cop

www.itu-cop-guidelines.com

karl.hopwood@eun.org