Swipe Safe
developed by ChildFund

ChildFund Australia

ONLINE SAFETY
BUILDING A SAFER FUTURE ONLINE

Date: 5 December 2024

Australian AID


Online Safety
VPN

Online protection refers to efforts aimed at ensuring the safety and well-being of individuals when engaging with digital environments.

THE INTERNET HAS BLURRED THE LINES BETWEEN OFFLINE AND ONLINE

EXAMPLES OF OFFLINE RISKS MANIFESTING ONLINE

1. **Exploitation and Abuse**
2. **Bullying**
3. **Fraud and Scams**
4. **Inappropriate Content**
5. **Misinformation and Radicalisation**

Why This Matters:

Online actions leave a digital footprint, making harm more permanent. Understanding that "offline risks can happen online" is crucial for creating effective safeguards that adapt traditional protection methods.

TYPES OF RISKS

Type	Definition
Content risks	A person engaged with or is exposed to potentially harmful content.
Contact risks	A person experiences or is targeted by contact in a potentially harmful adult-initiated interaction.
Conduct risks	A person witnesses, participates in or is victim of potentially harmful conduct. Typically, among peers.
Contract risks	A person is exploited by potentially harmful contract or commercial interests.

CHILDFUND SWIPE SAFE 6 KEY CONCEPTS

1. Public

Any information you post or share online, even if you do it privately, has the possibility to be publicly visible.

2. Permanent

Whatever we post on the internet can remain existing forever.

3. Connections

The internet allows us to connect with people all over the world, but not everyone is trustworthy.

4. Anonymity

People online can hide who they are. Some people might do this to trick or harm us.

5. Sources of Information

We have access to a lot of information, but it is important to think carefully about if it is true, accurate and reliable.

6. Respect

When engaging with people through screens, communication can feel less personal and less kind. It is important to remember that we are talking to people and to be respectful to others, and ourselves.

PUBLIC

- The internet is available to everyone.
- Everything we do online is potentially public.
- Setting privacy options can help, but it isn't perfect.

PERMANENT

- Everything on the internet is potentially permanent.
- Even if you delete a comment, post or picture from public view, it might still be findable.

CONNECTIONS

- Anyone in the world can potentially access the internet.
- We can communicate with people from different parts of the world at any time.
- Some people online try to do harm or take advantage of others.

ANONYMITY

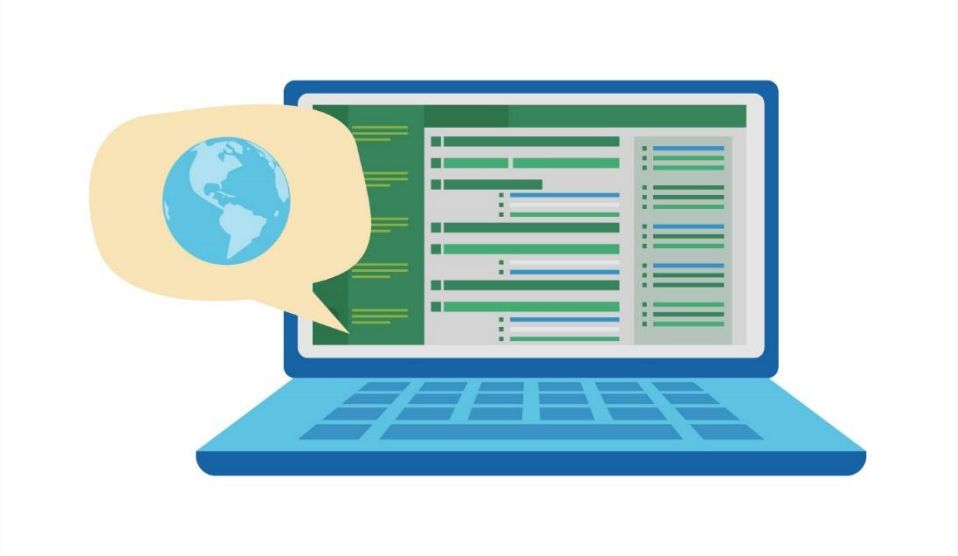
- You can never be 100% certain of who you are talking to online.

SOURCES OF INFORMATION

- There is a lot of information online.
- Working out information is true and reliable is getting harder.
- Searches provide the most *popular* results, not the most *correct!*
- AI and fake content: beyond text. It now includes fake photos, images, videos, and even songs.

RESPECT

- The rules of the real world exist in the online world too.
- If you wouldn't say it to a person's face, then don't say it online.



RISK MAPPING ACTIVITY

Type	Definition	Answer
Content risks	Young person engaged with or is exposed to potentially harmful content.	
Contact risks	Young person experiences or is targeted by contact in a potentially harmful adult-initiated interaction.	
Conduct risks	Young person witnesses, participates in or is victim of potentially harmful conduct. Typically, among peers.	
Contract risks	Young person is exploited by potentially harmful contract or commercial interests.	

Examples:

A. Sees violent images appearing in their Facebook feed.

B. Searches for and views pornography.

C. Repeatedly harassed by schoolmates via chat app.

D. Sent pornographic video by an adult.

E. Sent pornographic video by a girlfriend/boyfriend.

F. Sees advertising for gambling on their Instagram feed.

G. Asked in a game for private chat by an unknown person.

H. Tricked by an adult to send naked images.

I. Spends money on in-app purchases.

J. Clicks 'like' on a racist TikTok.

RISK MAPPING ACTIVITY

ChildFund

Type	Examples	Answers
Content risks	Violent, gory, hateful, extremist content. Pornographic or sexualized content.	B, J
Contact risks	Harassment, stalking, grooming, sexual extortion.	D, G, H
Conduct risks	Bullying, trolling, sexual messages, peer pressures, hate speech or harassment.	C, E
Contract risks	Poor platform design resulting in children open to harms like identity theft, fraud or scams.	A, F, I

Examples:

A. Sees violent images appearing in their Facebook feed.

B. Searches for and views pornography.

C. Repeatedly harassed by schoolmates via chat app.

D. Sent pornographic video by an adult.

E. Sent pornographic video by a girlfriend/boyfriend.

F. Sees advertising for gambling on their Instagram feed.

G. Asked in a game for private chat by an unknown person.

H. Tricked by an adult to send naked images.

I. Spends money on in-app purchases.

J. Clicks ‘like’ on a racist TikTok.

WHY YOUTH PARTICIPATION MATTERS?

Perspective and Relevance: Youth bring unique insights into their lived experiences, particularly in the digital world.

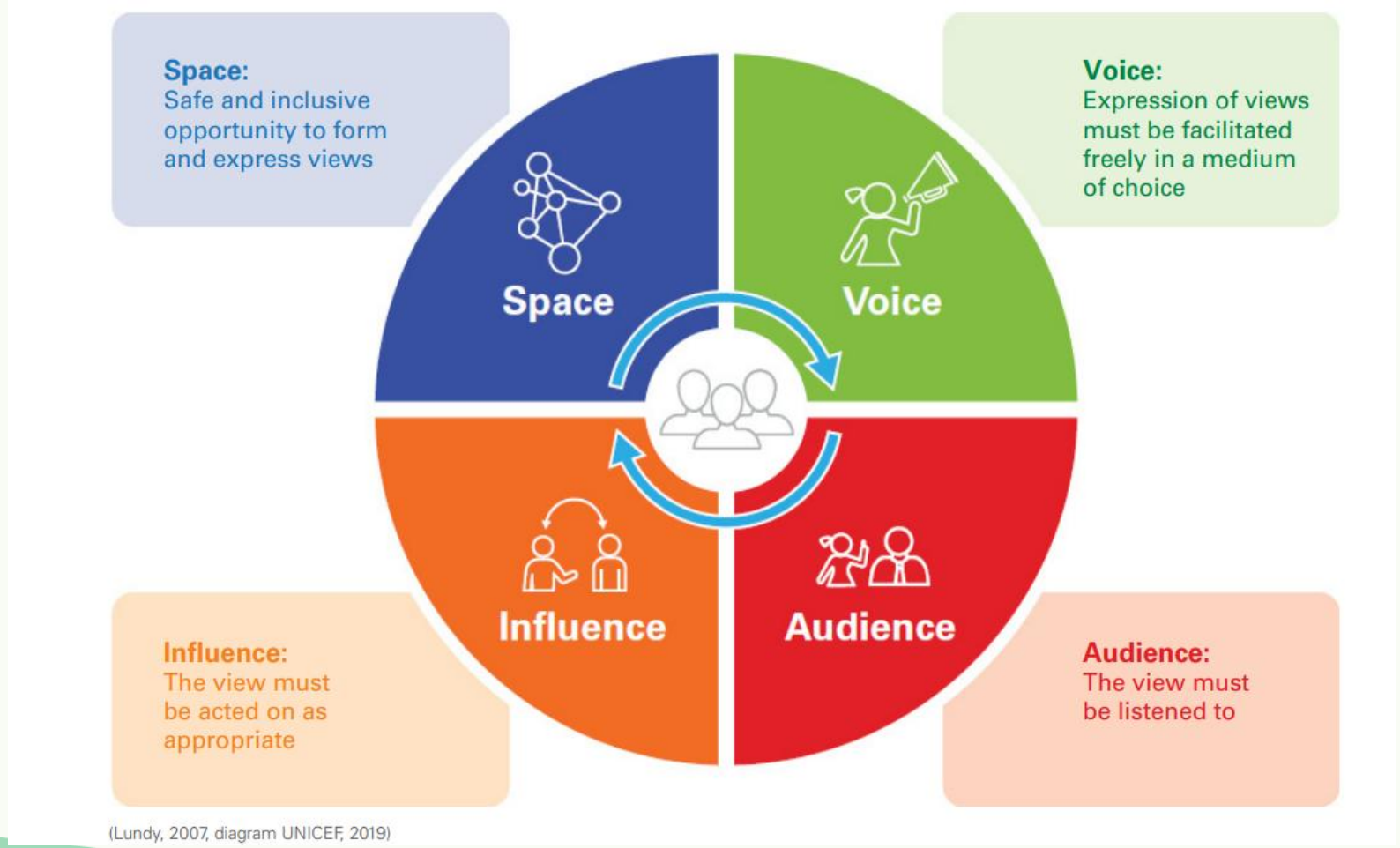
Innovation and Creativity: Young people often bring fresh ideas and innovative approaches, especially in tech-related areas.

Empowerment and Ownership: Participating in decision-making empowers youth by giving them a sense of agency.

Bridging Generational Gaps: Including youth fosters intergenerational dialogue, ensuring that older decision-makers better understand the challenges and opportunities faced by young people.

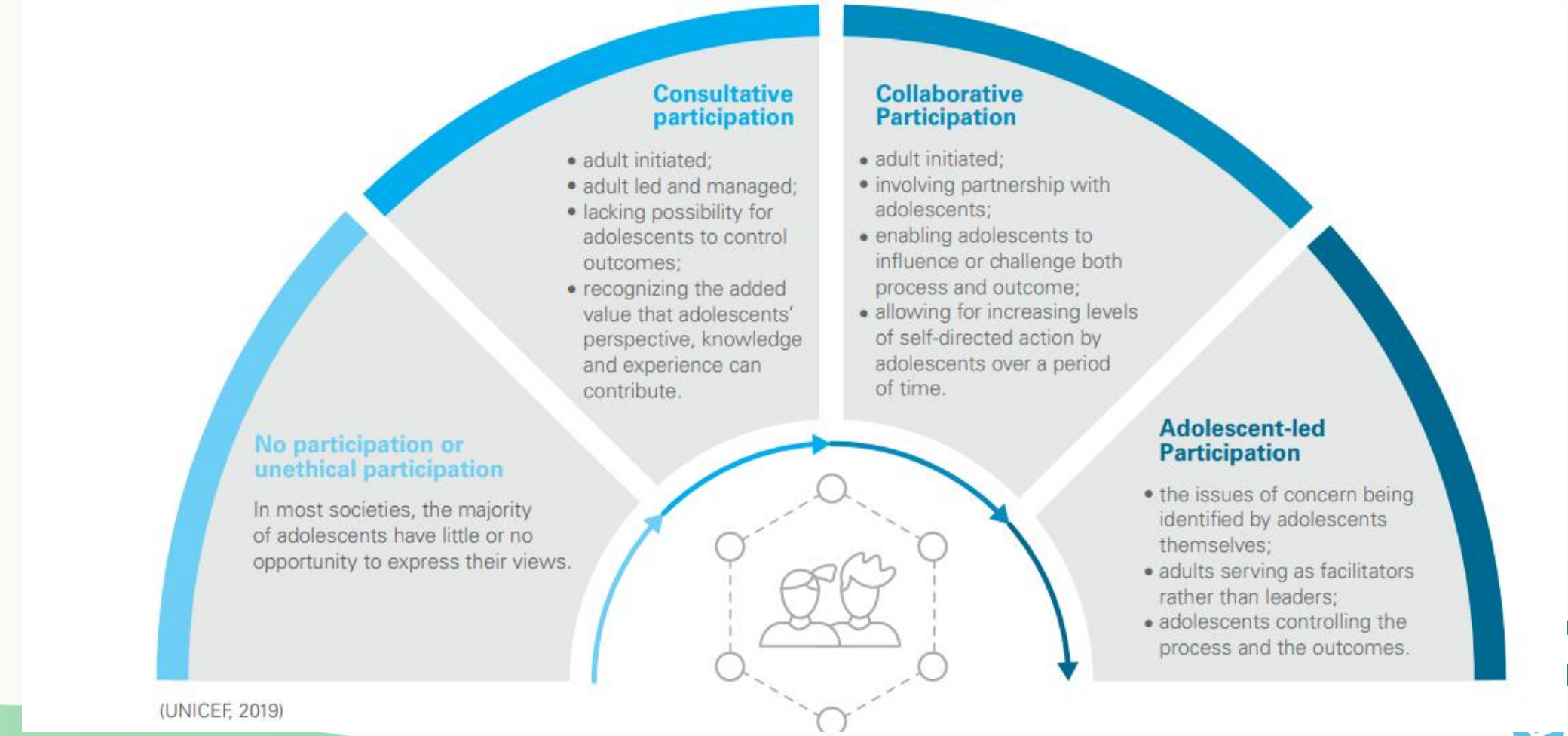
Sustainability: Engaging youth in policymaking builds a foundation for sustainable development.

FEATURES OF MEANINGFUL PARTICIPATION



(Lundy, 2007, diagram UNICEF, 2019)

MODES OF PARTICIPATION



(UNICEF, 2019)

YOUNG PEOPLE ARE PARTNERS AND CHANGE AGENTS WHO CAN POSITIVELY INFLUENCE THE MATTERS THAT AFFECT THEIR LIVES, BOTH INDIVIDUALLY AND COLLECTIVELY

CHILDFUND CHILD-CENTRED INDICATORS

Indicator	Detail Indicator	Explanation
Parental Monitoring of Online Activities	Do parents or caregivers regularly check what their children are doing online?	Evaluates how often parents or caregivers monitor their children's online activities to ensure safety.
Children's Ability to Identify Safe Online Behavior	Do children know how to block people and online content they don't want to see?	Measures children's knowledge and ability to block harmful content or users on digital platforms.
Reporting Harmful Online Content	Do children know how to report inappropriate, harmful, or illegal online content?	Assesses whether children are familiar with reporting mechanisms to address harmful online content.
Recognizing Trustworthy Information Online	Do children know what information to trust online?	Checks children's ability to discern between trustworthy information and misinformation on the internet.
Children's Awareness of Online Risks	Are children aware of the risks associated with online activities such as grooming, hacking, and scams?	Evaluates how aware children are of potential dangers online and their ability to recognize them.

Swipe Safe developed by ChildFund | ChildFund Australia

THANK YOU

GET IN TOUCH

If you would like to learn more, become a partner or join the program please visit SwipeSafe.org for more information.

You can always email us at SwipeSafe@childfund.org.au
or call us on **1800 023 600**

Australian AID