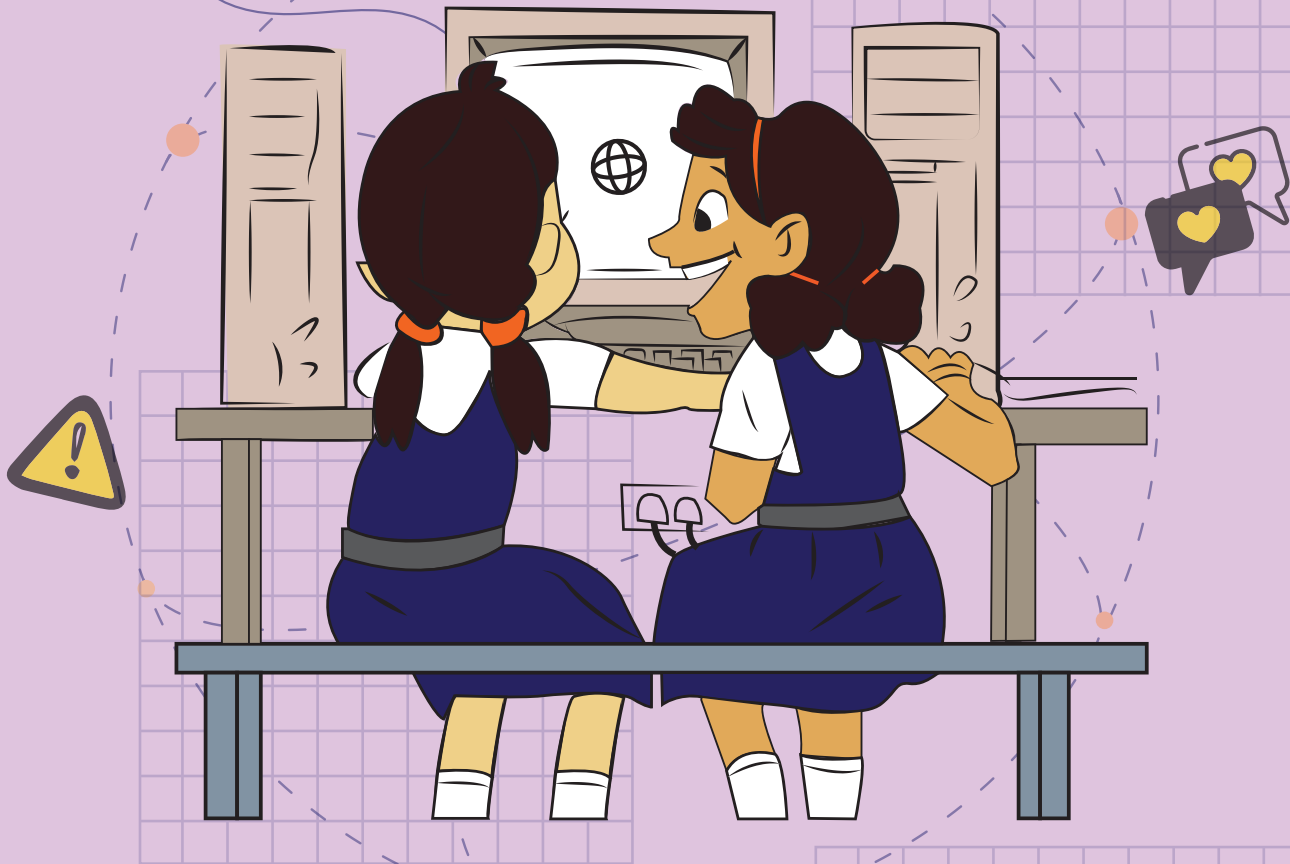# Be DigiSmart

DIGITAL LITERACY

Handbook

Save the Children

Yuvaa

INTRODUCTION

In an ever-increasing digital age, education, entertainment and experiences have moved online at breakneck speed. Over the past decade, while digital spaces have ensured enhanced connection for all populations, it has also exposed children and adults alike to new-age and hidden threats.

CHILDREN AND ADOLESCENTS UNDER 18 ACCOUNT FOR AN ESTIMATED ONE IN THREE INTERNET USERS AROUND THE WORLD.
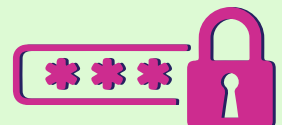
SOURCE: https://www.unicef.org/media/48601/file

This is the at-risk and most vulnerable group to cyber dangers especially in the absence of adequate awareness around cyber safety and digital rights as well as tools to address or deal with experiences of cyber threats.
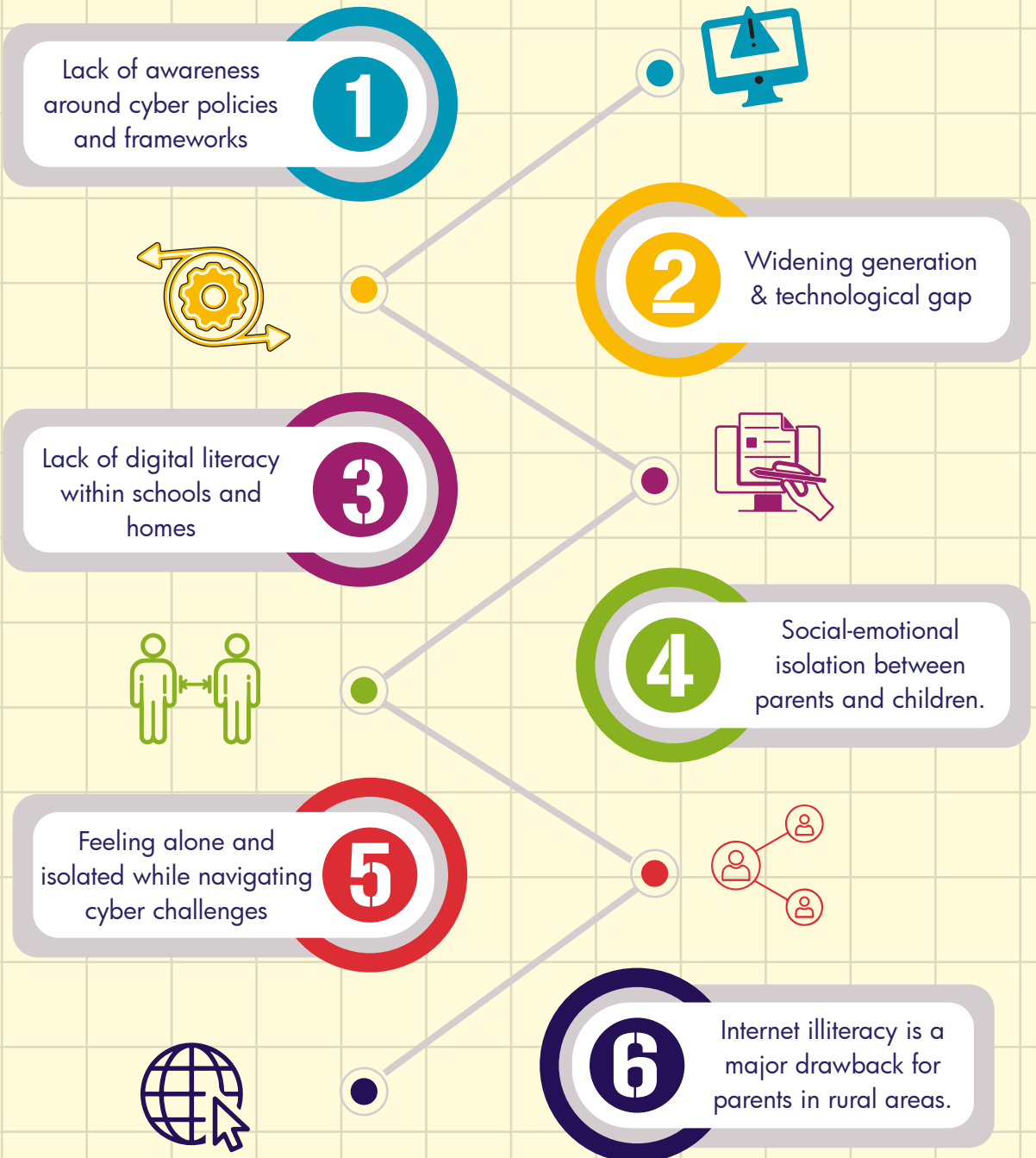
Children are the future building blocks of tomorrow. It is imperative for children, caregivers and duty-bearers to come together to address these concerns and ensure a safe cyber experience for children online through awareness generation, advocacy and capacity building.

Caregivers are seen as compassionate allies in an attempt to foster better experiences for children online. In addition to this, young adults a.k.a Gen-Z Netizens can also become torch bearers and agents of change to pave the way for a safer internet for children.

WHAT ARE THE CHALLENGES CHILDREN AND CAREGIVERS FACE?

1 Lack of awareness around cyber policies and frameworks

2 Widening generation & technological gap

3 Lack of digital literacy within schools and homes

4 Social-emotional isolation between parents and children.

5 Feeling alone and isolated while navigating cyber challenges

6 Internet illiteracy is a major drawback for parents in rural areas.
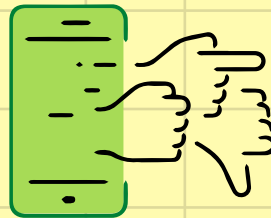
MAJOR CYBER THREATS REPORTED

FINANCIAL FRAUD AND SCAMS

*PHISHING AND FAKE CONTENT

MORPHING AND GROOMING

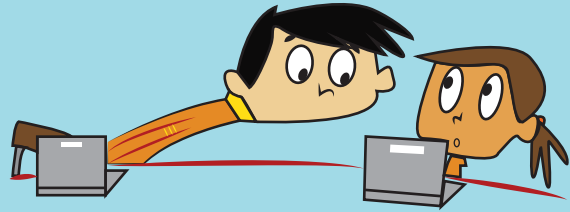CYBERBULLYING AND HATE SPEECH

IDENTITY THEFT AND DOXING*

SMARTPHONE ADDICTIONS

*DOXING: Cyber security company Kaspersky defines doxing as the act of revealing identifying information about someone online, such as their real name, home address, workplace, phone, financial, and other personal information. That information is then circulated to the public — without the victim's permission.

*PHISHING: According to software company Imperva, Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. The attacker usually masquerades as a trusted entity.
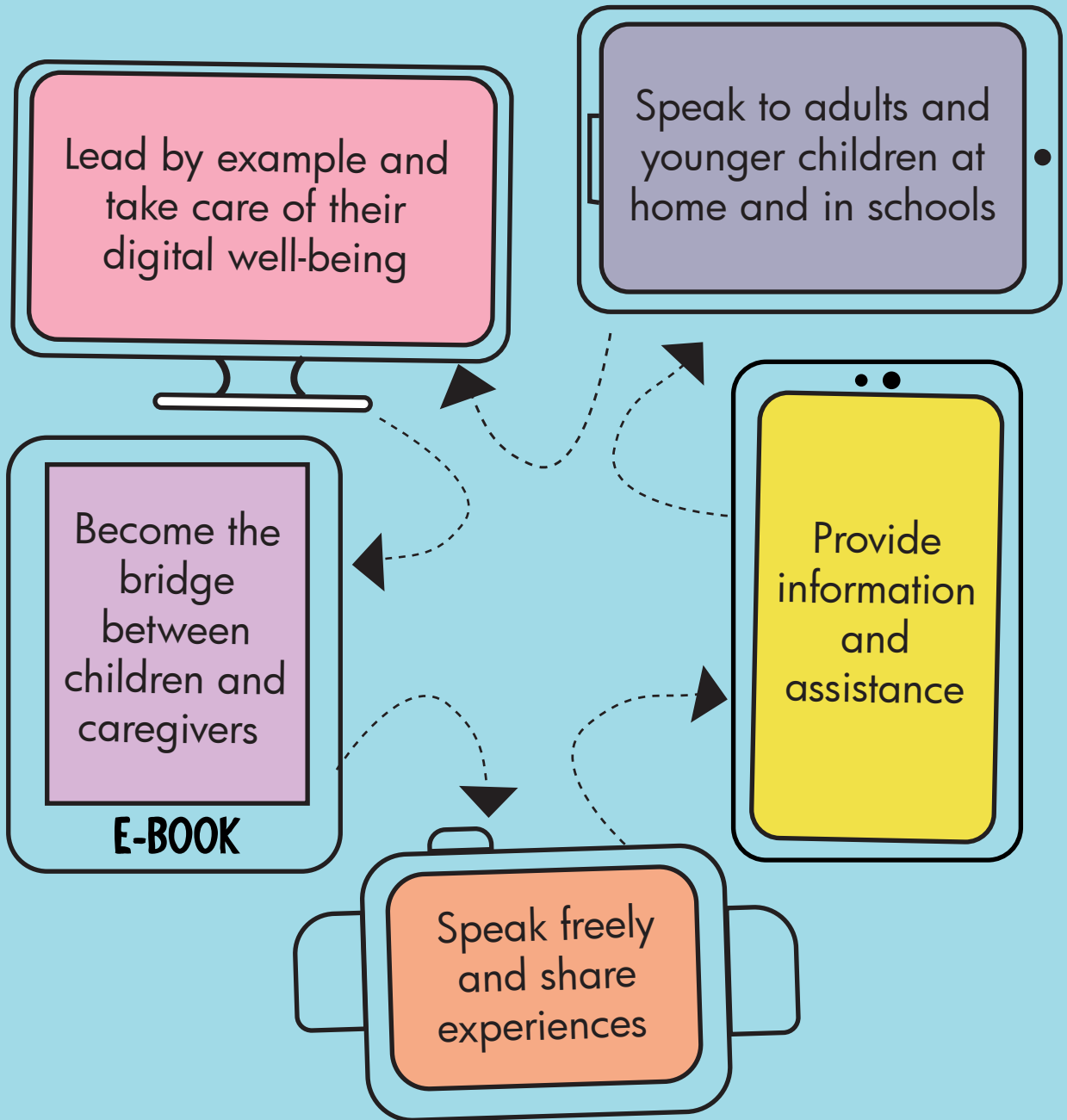
HOW CAN CAREGIVERS ALLY UP FOR SAFE INTERNET FOR CHILDREN?

IT IS IMPORTANT FOR BOTH PARENTS AND TEACHERS TO STAND SIDE BY SIDE WITH CHILDREN FOR REMOVING BARRIERS FOR THEIR SAFE ONLINE EXPERIENCES.
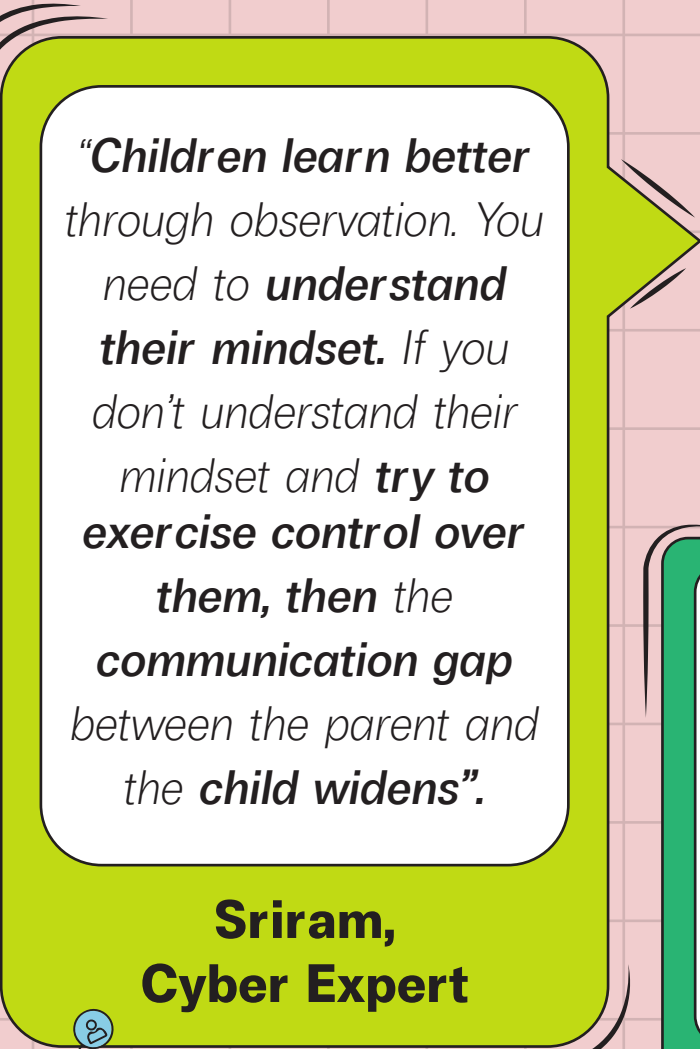
Encouraging preventive and responsive digital behaviour

Having dedicated timings for Smartphone use at home

Non-controlling and non-judgemental caregiving

Setting rules and guidelines but not become controlling.

Leading by example and following digital guidelines themselves.

HOW NETIZENS CAN INSPIRE COLLECTIVE ACTION

Lead by example and take care of their digital well-being

Speak to adults and younger children at home and in schools

Become the bridge between children and caregivers

E-BOOK

Provide information and assistance

Speak freely and share experiences

EXPERT THOUGHTS

*"The reason why **cybercrimes** keep on increasing is because **nobody wants to report** them to the competent authorities."*
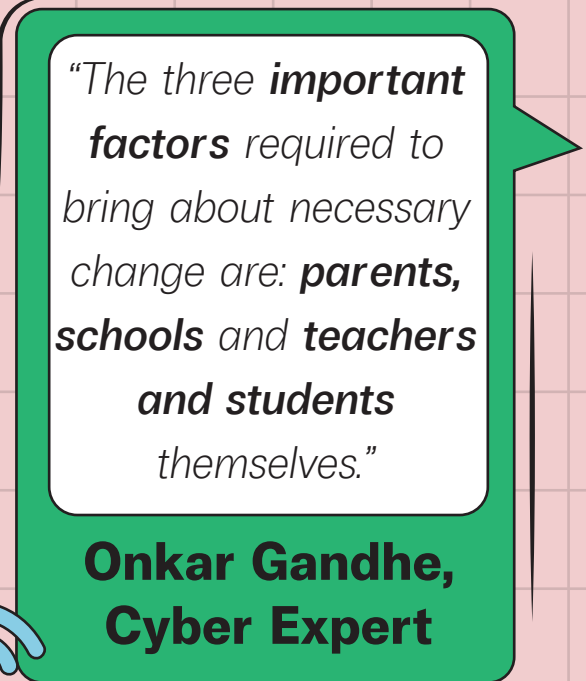
Sriram, Cyber Expert

*"**Children learn better** through observation. You need to **understand their mindset.** If you don't understand their mindset and **try to exercise control over them, then** the **communication gap** between the parent and the **child widens".**
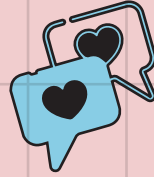
Sriram, Cyber Expert

*"The three **important factors** required to bring about necessary change are: **parents, schools** and **teachers and students** themselves."*

Onkar Gandhe, Cyber Expert

"*We feel safe* using the internet because *we only watch useful content.* We don't watch unwanted content online."
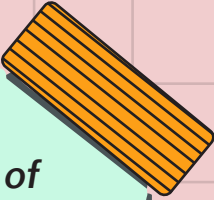
PRUDHVI, 11 YEARS
Student of PUMS, Vengathur

"*I fear answering unknown numbers* because they might *trace my phone.*"

KALYAN, 12 YEARS
Student of PUMS, Kilnallathur

"*Getting lots of unwanted links*, and unknowingly clicking on it *makes me feel unsafe* on the internet."

MEENAKSHI, 10 YEARS
Student of PUMS, Kilnallathur

"*Cell Phone addiction* is a *huge issue. Children bring* them to schools & *inside classes.*"

SHANTI, 41 YEARS
Teacher at GHS, Kilambakkam

TIPS FOR CHILDREN AND CAREGIVERS

Don't share private information

Fact Check before sharing sensitive information

Seek consent when using other devices

Check privacy settings on mobile, apps and browsers

Don't download fishy links or games

Don't connect to an unknown or unrecognised wireless access point.

Use known Wi-Fi links, which are password protected.

Disable Bluetooth when not in use

Regularly update software and operating systems

Keep computer/mobile cameras covered when not in use as they are prone to hacking

Install anti-virus software and ensure that it's updated from time to time.

Take screen breaks often

WHEN FACING CYBER CHALLENGES OR THREATS

BE EMPATHETIC ONLINE

DON'T WORRY OR STRESS

KNOW YOU'RE NOT ALONE

ASK YOUR TEACHERS

Online

DON'T BE SHY TO SHARE

TALK TO YOUR PARENTS / CHILDREN

SEEK HELP FROM SENIORS / PROFESSIONALS OR OTHER NETIZENS

CHANNELS OF REPORTING

WARNING!

Attention Please

_____
_____

NATIONAL CYBER CRIME REPORTING PORTAL

This portal is an initiative of the Government of India to facilitate victims of cyber crime with reporting complaints. It places special focus on cyber crimes against women and children. To report cyber crimes, visit

(https://cybercrime.gov.in/)

NCPCR

NATIONAL COMMISSION FOR PROTECTION OF CHILD RIGHTS

Protection of Children from Sexual Offences (POCSO) e-Box is an online complaint box for reporting child sexual abuse. It is an initiative of the National Commission for Protection of Child Rights (NCPCR) to help children report such crimes directly to the Commission.

(https://ncpcr.gov.in/index2.php)

CHILD LINE 1098 NIGHT & DAY

CHILDLINE 1098

India's first 24-HOUR,
free, emergency phone service for children in need of aid and assistance. They not only respond to the emergency needs of children but also link them to relevant services for their long-term care and rehabilitation.

KNOW YOUR
LAWS AND DIGITAL RIGHTS

There are many legal frameworks in place for ensuring cyber safety. To inspire real progress, it is important to report cyber crimes and address the issues on the frontlines in a collaborative approach that involves caregivers and duty bearers.

INDIAN PENAL CODE is the main criminal code for the country. Section 378 of the IPC relating to "theft" of movable property will apply to the theft of any data, online or otherwise.

INFORMATION & TECHNOLOGY (IT) ACT provides legal recognition to the transaction done via electronic exchange of data and other electronic means of communication. Sections 43 and 66 of the IT Act penalize a number of activities: hacking into a computer network, data theft, denying an authorized personnel access to a computer.
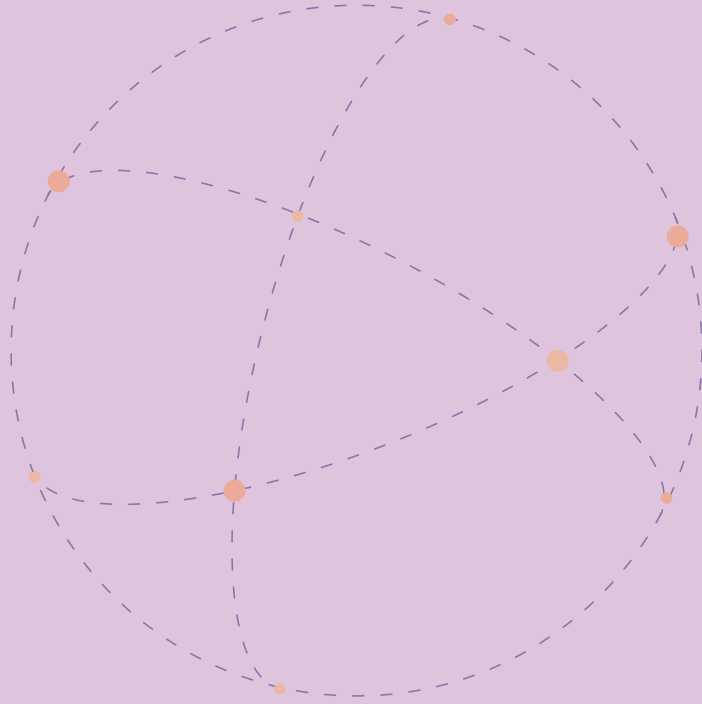
LEGAL FRAMEWORKS FOR CYBER SAFETY OF CHILDREN

(POCSO) PROTECTION OF CHILDREN FROM SEXUAL OFFENCES ACT seeks to provide stringent punishment to those engaging in sexual crimes against children.

THE JUVENILE JUSTICE ACT pertains to provisions for children found in conflict with the law in India. It also gives provisions for children in need of care and protection.

THE NATIONAL COMMISSION FOR THE PROTECTION OF CHILD RIGHTS provides speedy trial of offenses against children or of violation of child rights and for matters connected therewith or incidental thereto. https://www.ncpcr.gov.in/

Save the Children

in Collaboration with