Call for Inputs on digital education for young people

Civil Society's Reply from India

Input details:

Ten inputs provided by groups or individuals from different states/areas of India

1. Details of the respondent

Respondent profile: Young person (18-35)
Gender: Female
On behalf of: Adolescent girls
Country: India
Organization: Our Lady of Charity of The Good Shepherd (RGS)

1) What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

- Students from vulnerable groups have low access to online education because of limited resource bases—do not have proper Internet access.
- Face difficulties in learning new technology and confused to operate.
- Unable to understand the directions during online learning, feel disinterested.
- Difficulties in completing the assignments/work.
- Sometimes get distracted with social media and internet notifications while accessing.
- Girls specifically have less access to the internet. The digital divide in education is seen more.

2) What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of specific laws and regulations, measures, policies, and programmes directed at ensuring young people's universal access to digital education.

- The government of Andhra Pradesh, India has emphasized the integration of Information and Communication Technology (ICT) in schools. It aims to provide digital infrastructure, including computer labs, internet connectivity, and digital learning resources, to enhance the teaching and learning experience.

- DIKSHA (Digital Infrastructure for Knowledge Sharing) is a national platform for school education in India. It is an initiative of the National Council for Educational Research and Training (NCERT), under the Ministry of Education.
- DIKSHA is the 'One nation: One digital platform' for school education in India. Digital Infrastructure for Knowledge Sharing (DIKSHA) portal and mobile app created by Moe is a storehouse of a large number of e Books and e-Contents created by States/UT's and National level organizations.

3) What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?

- To overcome the digital divide Andhra Pradesh had given 18270 tablets to 609 school students and 2850 laptops to 95 school students at Secondary schools.
- PM e Vidya: A comprehensive initiative called PM e Vidya is launched as a part of the Atma Nirbhar Bharat Programme, which unifies all efforts related to digital/online/on-air education to enable coherent multi-mode access to education. Initiatives include :
    - DIKSHA is the nation's digital infrastructure for providing quality e-content for school education in states/ UT's: and QR coded Energized Textbooks for all grades (one nation, one digital platform)
    - Access through TV channels: One earmarked TV channel per class from 1 to 12 (One class, One channel)
    - Extensive use of Radio, Community radio, and CBSE Podcast- Shiksha Vani
    - Special e-content for visually and hearing impaired developed on Digitally Accessible Information System (DAISY) and in sign language on NIOS website/ YouTube
- National Digital Education Architecture (NDEAR) has been conceived as a unifying National Digital infrastructure to energize and catalyse the education ecosystem. The core idea of NDEAR is to facilitate achieving the goals laid down by National Education Policy 2020, through a digital infrastructure for innovations by, through and in the education ecosystem, ensuring autonomy and participation of all the relevant stakeholders.
- The Department of School Education of Andhra Pradesh adopted several innovative initiatives during the COVID-19 pandemic. To bridge the gap, many surveys, and online training were conducted for building capacities of teachers and students. The following digital initiatives have been implemented in the state to promote learning and to provide support to students for continuing their learning systematically.
- Vidya Varadhi T.V Lessons:
- It is broadcasted through Doordarshan for class 1 to 10th Students in all subjects by subject experts, with the objectives of providing learning opportunities to students, recapitulating concepts and bridging the learning gaps during the closure of schools in the COVID-19 pandemic. This was scheduled from 10th June 2020 to January 31st 2021.
- A National Initiative for school Heads and teachers for Holistic Advancement of the elementary stage under Samagra Shiksha was launched. It is a flagship program of MHRD. The first pilot of NISHTHA online was undertaken in Andhra by NCERT.

Therefore, Andhra Pradesh is the pioneering state in the country in conducting the online NISHTHA training of NCERT.

- Andhra Pradesh state has conducted 90 days of NISHTHA online courses with 18 modules (Courses) duly providing live classes and collecting portfolios through the online cloud. A dashboard is also provided to teachers to check their submitted portfolios. 1,03,897 teachers are pursuing primary level training; out of these 97,894 teachers have completed all the modules and have been awarded online certificates through the DIKSHA platform. Online training for teachers on School Safety, Health and Teaching aptitude levels: The Government of A.P has initiated a school safety program through virtual mode in all elementary and secondary schools to bring awareness on school safety in the post-Covid-19 scenario. E- Modules based on school safety were prepared and made available on the DIKSHA platform. Poster and pamphlets are printed and displayed in the schools on the School safety program. “We love reading” virtual orientation to stakeholders. ● The state launched the “We Love Reading” Campaign in all schools for the improvement of reading as part of the development of foundational literacy skills, the virtual orientation sessions are available on the DIKSHA platform. the state has planned to establish 1000 model libraries and designed to digitalize the libraries.

- Bridge course material
- Online learning through Whats App groups
- Identification of children with and without access to technological devices
- Zoom class for students for better understanding of critical topics
- Monitoring of student’s attendance through the app
- Conduct of language festivals through virtual mode

4) What are the main gaps and challenges to young people’s protection from online threats in law, policy, and practice in your country and the impacts on young people’s human rights? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

- Inappropriate and unsuitable content for children
- Cyber-predators and cyber-bullying
- Online scams

5) What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.

The legal and policy framework for handling issues of Child Online Protection in India include:

- Constitution of India, National Policy for Children (NPC), 2013 National Policy on ICT in Schools, 2012, Draft National Education Policy, 2019, National Cyber Security Policy, 2013, Indecent Representation of Women (Prohibition) Act, 1986, and Protection of Children from Sexual Offences (POCSO) Act, 2012.

Government has taken several steps to be implemented by Internet Service Providers (ISPs) to protect children from sexual abuse online. These include:

- Government blocks the websites containing extreme Child Sexual Abuse Material (CSAM) based on INTERPOL's "Worst-of-list" shared periodically by Central Bureau of Investigation (CBI) which is the National Nodal Agency for Interpol. The list is shared with Department of Telecommunications (DoT), who then directs major ISPs to block such websites. Government ordered major Internet Service Providers (ISPs) in India to adopt and disable/remove the online CSAM dynamically based on Internet Watch Foundation (IWF), UK list. Ministry of Electronics and Information Technology (MeitY) has implemented a major programme on Information Security Education and Awareness (ISEA). A dedicated website for information security awareness (https://www.infosecawareness.in) has also been set up.

2. Details of the respondent

Respondent profile: Educator
Gender: Female
On behalf of: Educators and Adolescent girls
Country: India
Organization: IIMA India

1) What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

The digital education divide between rural and urban areas is significant. More than half of the Indian population does not have access to the internet, and underprivileged communities are still lagging in the digital race. A study by the Azim Premji Foundation in 2021 showed that almost 60 per cent of school children in India cannot access online learning opportunities. The economically backward families struggle to have 2 full meals and a safe shelter. A digital device like mobile, laptop etc with internet access is an unaffordable luxury. The digital divide in Indian schools is a growing concern that is primarily caused by economic and social factors. According to UNESCO, only 8% households in India have access to a computer, and only 15% have access to the internet. This lack of access to technology has a direct impact on the education system, where students from low-income families are at a disadvantage.

Apart of individual students who face the challenges, lack of infrastructure is one of the prominent factors contributing to the digital divide especially in the rural areas in India as schools in these areas lack basic facilities like electricity, which makes it difficult to provide access to technology. Additionally, the cost of technology remains high, making it difficult for schools to provide access to students from low-income families.

The digital divide has a significant impact on the quality of education in Indian schools. Students who do not have access to technology are at a disadvantage and are unable to compete with their peers who have access to technology. This can lead to lower academic performance and a lack of interest in education.

Moreover, the lack of access to technology also affects the quality of teaching. Teachers who do not have access to technology are unable to keep up with the latest teaching methods

and tools, which can lead to a lack of engagement and interest among students. ***(Ref:https://aif.org/digital-education-in-india-avenues-and-challenges/)***

2) What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of specific laws and regulations, measures, policies, and programmes directed at ensuring young people's universal access to digital education.

The government of India is imagining and shaping E-learning with digital pedagogy as a long-term strategy in the Education sector. It has contributed to the new age of learning which is not restricted to schools. Today the Ministry of Education is working upon the concept of learning by all, with all, and for all under the framework to adapt the enhanced learning experience for the students.

Government Initiatives for Digital Education in India

The Ministry of Education in India has undertaken many initiatives to promote digital education. Here are some key initiatives:

SWAYAM (Study Webs of Active Learning for Young Aspiring Minds) is an online platform offering free courses from elementary to postgraduate levels. It provides access to high-quality study material, video lectures, and interactive quizzes.

National Digital Library (NDL) is a digital repository of educational resources. This includes textbooks, articles, audiobooks, videos, and lectures. It offers a vast collection of learning materials for students and teachers.

e-Pathshala is an online portal and mobile app. It provides access to textbooks, audio, video, and multimedia educational content. Content is available for school students from Class 1 to Class 12 in many languages.

DIKSHA is a national digital platform. It hosts e-learning content for school students, teachers, and parents. It offers interactive lessons, worksheets, and assessments aligned with the school curriculum.

National Repository of Open Educational Resources (NROER) is a digital platform that curates and shares open educational resources. It provides a wide range of digital content. This includes textbooks, lesson plans, multimedia materials, and teaching aids.

Virtual Labs. The Virtual Labs initiative aims to provide remote access to labs for students and researchers. It offers a simulated learning environment. The users can perform experiments and gain practical knowledge.

National Programme on Technology Enhanced Learning (NPTEL) provides online courses and study materials in various disciplines. This includes engineering, science, humanities, and management. It is a joint initiative of the Ministry of Education and IITs.

Pragyatah is a set of guidelines developed by the MoE to help schools use digital technology. The guidelines cover a range of topics. This includes the use of technology for teaching and learning and the management of digital resources.

For the differently-abled

- Sign Language Channel: A dedicated DTH channel with sign language is available for hearing-impaired students. It provides accessibility and supports their learning needs.

- Digitally Accessible Study Material: The study material has been developed in Digitally Accessible Information System (DAISY) format. This can aid hearing and visually impaired students.

Radio Broadcasting

- Activity-based Learning: Radio broadcasts focus on activity-based learning methods. This interactive approach engages students and promotes effective learning.

- Community Radio Stations: 289 community radio stations are utilized for this purpose. They broadcast content related to the National Institute of Open Learning (NIOS) for grades 9 to 12. This enables students in remote areas to access educational content.

- Remote Area Education: Radio broadcasting is particularly beneficial for students residing in remote areas. This is especially for grades 5 to 1. It helps bridge the education gap. It provides learning opportunities to those with limited access to traditional education.

- Shiksha Vani Podcast: Shiksha Vani is a podcast by the Central Board for Secondary Education (CBSE). It is utilized by learners from grades 12 to 9. Shiksha Vani offers over 430 audio content pieces. It covers all subjects from grades 1 to 12. It facilitates learning through audio-based resources.*(Ref: https://testbook.com/ias-preparation/digital-education-in-india)*

3) What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?

India has a fairly comprehensive policy and legal framework addressing rights and protection for children, providing opportunities to ensure that all children have equal access to quality protection services. The core child protection legislation for children is enshrined in four main laws: The Juvenile Justice (Care and Protection) Act (2000, amended in 2015); The Prohibition of Child Marriage Act (2006); The Protection of Children from Sexual Offences Act (2012), and The Child Labour (Prohibition and Regulation) Act (1986, amended in 2016). Over the past five years, notable efforts have been made to set up fast track courts and deal with cybercrime against children and women. In 2019, the Protection of Children from Sexual Offences Bill was amended, stipulating stricter punishment for sexual crimes against children.
In 2019, the government launched the National Cybercrime Reporting Portal for the public to report instances of cybercrime, with a special focus on those committed against women and children. The National Commission of Protection of Child Rights (NCPCR) has established an online complaint management system that enables a confidential platform for victims (or their representatives) to report cases of child abuse and sexual assault. The Ministry of Home Affairs has sanctioned a 'Cyber Crime Prevention against Women and Children (CCPWC)' scheme which comprises an online cybercrime reporting portal for cases of Child Pornography/

Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content. Steps for spreading awareness have been taken through alerts and advisories, training of law enforcement agencies, improving cyber forensic facilities etc. ***(Ref: https://timesofindia.indiatimes.com/blogs/voices/the-necessity-of-child-safety-policies-and-regulations-in-online-education/)***

4) What are the main gaps and challenges to young people's protection from online threats in law, policy, and practice in your country and the impacts on young people's human rights? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

India has witnessed a whopping 50% of internet penetration in 2020 as against 34.4% in 2019, predominantly as an after-effect of the pandemic. The surge in online activity by children, therefore, becomes apparent as out of India's 749mn internet users, 232mn are children. The internet serves as a double-edged sword with enabling connectivity, access to knowledge, and entertainment on one hand and potential exposure to harmful and inappropriate content on the other. Children, as sensitive and impressionable individuals, must be protected from possible detriments to internet usage. Cyberbullying, cyber sexual harassment, cyber grooming, loss of privacy, and enticement to illegal behavior are only a few dangers to name. The increasing number of children persistently using social media to record and share their life through photographs and videos necessitates certain regulations and mechanisms to monitor children's online activities, reduce risks and vulnerabilities, and protect them from harm.

Teachers, parents, and students alike navigate through an unknown virtual world to maintain an education system. Due to this unprecedented rise in online communication and screen time, children are left more vulnerable to online exploitation. The pandemic also broadened the avenue of digital learning and the subsequent growth of EdTech companies. This growth has unfortunately manifested data protection risks and privacy breaches. If left unchecked, the digitalization of education may have seriously damaging repercussions.

Hence Government must engage in endeavors to raise awareness on the matter and insists digital education promoting companies/agencies to build products that cater to the specificities of the issue and advocate robust legal and redressal mechanisms in cases of violation of online child safety. ***(Ref.https://www.livemint.com/opinion/columns/our-new-digital-rules-must-ensure-online-child-safety-11681836313154.html)***

5) What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.

There are various laws that mention monitoring, detection, prevention, mitigation and management of Incidents. The salient ones are as follows:

The IT Act along with its allied Rules is the primary law dealing with the varied aspects of how to look at issues related to electronic records and documents, digital signatures, and cybercrime on information, systems etc. The Act also prescribed the offences and fines. Over a period of time the changing technology landscape brought about an amendment in this Act, which is the IT Amendment Act. This further enhanced the scope of

cybercrimes and introduced penalties for offences related to data breaches, identity theft, and online harassment.

As per the IT Act, the Computer Emergency Response Team – India (CERT-In) provides guidelines for monitoring, detecting, preventing, and managing cybersecurity Incidents.

As per this, service providers, intermediaries, data centres, body corporates, and Government organisations are obligated to take specific actions or provide information for cyber Incident responses, as well as for protective and preventive measures against cyber Incidents.

National Cyber Security Policy 2023: The objective of this policy is to safeguard both information and the infrastructure in cyberspace. It seeks to establish the capabilities needed to prevent and respond effectively to cyber threats, as well as to minimise vulnerabilities and mitigate the impact of cyber Incidents.

This will be achieved through a combination of institutional structures, skilled individuals, established processes, advanced technology, and collaborative efforts.

The policy is designed to instil a high level of trust and confidence in IT systems. It also aims to fortify the regulatory framework to ensure security and bolster the safeguarding and resilience of the nation's critical information infrastructure (CII).

This will be accomplished by the operation of a 24/7 National Critical Information Infrastructure Protection Centre (NCIIPC) and the enforcement of security practices pertaining to the design, procurement, development, utilisation, and operation of information resources.

Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 In 2021, India implemented regulations commonly referred to as the Intermediary Rules. These guidelines establish a legal structure governing social media platforms, over-the-top (OTT) platforms, and digital news providers. Additionally, they encompass clauses pertaining to safeguarding data and addressing complaints.

The DPDPA is an Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes. It has a clear mandate for reporting Incidents and fines for not following said mandates.

There is also the upcoming Digital India Act; the Government is presently looking to replace the IT Act with the Digital India Act, which will deal with online safety, trust and accountability, open internet, and regulations of new age technologies like artificial intelligence and blockchain technologies.

The Indian Penal Code also has provisions related to cyber-incidents, although this must be read with the IT Act.

The Central Government launched a National Cyber Crime Reporting Portal, [Hyperlink], to enable citizens to report complaints pertaining to all types of cybercrimes, with a special focus on cybercrimes against women and children.

The Government is also operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre), which provides the detection of malicious programs and free tools for cleaning malicious code as well as tools such as M-Kavach for addressing threats related to mobile phones.

The CERT-In coordinates with its counterpart agencies in foreign countries on cyber Incidents originating outside the country. ***(Ref: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india#)***

3. Details of the respondent

Respondent profile: Educator
Gender: Female
Country: India
Organization: IIMA India

1) What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

- **Lack of internet connectivity:** There are many places in India, particularly the remote areas, which lack internet connectivity. This is a great hindrance in accessing digital education to thousands of youth
- Young people from **poor economic background** cannot afford digital devices and technology as these are expensive
- Only technically sound youth have opportunities for digital education
- Misuse of the digital gadgets as a result of ignorance and misinformation
- Young people lose their career due to addiction to digital devices
- Increase in suicide rate among the young people

2) What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of specific laws and regulations, measures, policies, and programmes directed at ensuring young people's universal access to digital education.

Digital Education in India. Digital education is essentially the future of education all over the world, and the same applies to India as well. This is a Revolutionary initiative that will help millions of people, especially school-going students, in attaining knowledge and shaping a better future for themselves. Looking at the broad and immense future of Digital Education Technology, the Government of India is promoting digital education very aggressively and is trying to make sure of its universal availability throughout the country.

The Digital India Campaign of the Government of India is also playing an anchor role in the spread of digital education.

Government Initiatives for Digital Education in India

The Ministry of Education in India has undertaken many initiatives to promote digital education. Here are some key initiatives:

1. SWAYAM (Study Webs of Active Learning for Young Aspiring Minds): It is an online platform offering free courses from elementary to postgraduate levels. It provides access to high-quality study material, video lectures, and interactive quizzes.
2. National Digital Library (NDL): The NDL is a digital repository of educational resources. This includes textbooks, articles, audiobooks, videos, and lectures. It offers a vast collection of learning materials for students and teachers.
3. e-Pathshala: e-Pathshala is an online portal and mobile app. It provides access to textbooks, audio, video, and multimedia educational content. Content is available for school students from Class 1 to Class 12 in many languages.
4. DIKSHA: DIKSHA is a national digital platform. It hosts e-learning content for school students, teachers, and parents. It offers interactive lessons, worksheets, and assessments aligned with the school curriculum.
5. National Repository of Open Educational Resources (NROER): NROER is a digital platform that curates and shares open educational resources. It provides a wide range of digital content. This includes textbooks, lesson plans, multimedia materials, and teaching aids.
6. Virtual Labs: The Virtual Labs initiative aims to provide remote access to labs for students and researchers. It offers a simulated learning environment. The users can perform experiments and gain practical knowledge.
7. National Programme on Technology Enhanced Learning (NPTEL): NPTEL provides online courses and study materials in various disciplines. This includes engineering, science, humanities, and management. It is a joint initiative of the Ministry of Education and IITs.
8. Pragyatah: Pragyatah is a set of guidelines developed by the MoE to help schools use digital technology. The guidelines cover a range of topics. This includes the use of technology for teaching and learning and the management of digital resources.
9. For the differently-abled

- **Sign Language Channel: A dedicated DTH channel with sign language is available for hearing-impaired students. It provides accessibility and supports their learning needs.**

- **Digitally Accessible Study Material:** The study material has been developed in Digitally Accessible Information System (DAISY) format. This can aid hearing and visually impaired students.

10. Radio Broadcasting

- **Activity-based Learning:** Radio broadcasts focus on activity-based learning methods. This interactive approach engages students and promotes effective learning.

- **Community Radio Stations:** 289 community radio stations are utilized for this purpose. They broadcast content related to the National Institute of Open Learning (NIOS) for grades 9 to 12. This enables students in remote areas to access educational content.

- **Remote Area Education:** Radio broadcasting is particularly beneficial for students residing in remote areas. This is especially for grades 5 to 1. It helps bridge the education gap. It provides learning opportunities to those with limited access to traditional education.

- **Shiksha Vani Podcast:** Shiksha Vani is a podcast by the Central Board for Secondary Education (CBSE). It is utilized by learners from grades 12 to 9. Shiksha Vani offers over 430 audio content pieces. It covers all subjects from grades 1 to 12. It facilitates learning through audio-based resources.

3) What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?

India is home to a population which is rooted in diverse socio-economic backgrounds. As per the living standards of people, a wide range of devices are in use - from high-end secured electronic devices to low-cost mobile phones. This makes it difficult for authorities to set uniform legal and technical standards for regulating data-protection. Additionally, digital literacy and awareness among the population is also very low.

India does not yet have a comprehensive law governing the data privacy of citizens. The provisions available in this regard are few, some vague, and scattered across case laws and other legislations. The **Information Technology (IT) Act was passed in 2000** to deal with cybercrime and electronic commerce in India but it doesn't address privacy issues and doesn't deal with nuances of cybersecurity. In 2021, the IT Rules were introduced but it doesn't protect data of social media users from the government and thus makes the ruling party an arbiter to suppress speech as they feel right. The rules allow overboard grounds for restricting online content and require messaging services to violate "end to end encryption" when needed by the government. Important case law in this regard is the landmark Puttaswamy vs. Union of India case (2017) which held that the Right to Privacy was a fundamental right of citizens and also laid down certain provisions regarding the privacy of children online but didn't provide enough tools to ensure how data privacy should be prioritized. However, even when we look at these three together, they are not adequately detailed to cover all aspects of digital privacy and the online safety of citizens. In this context, in 2019, a new Personal Data Protection (PDP) Bill was proposed by the Parliament which, among other provisions, proposes setting the age of digital consent to 18 and requiring

parental consent for all data collection and processing for individuals under that age but the proposed bill too has its own set of flaws.

4) What are the main gaps and challenges to young people's protection from online threats in law, policy, and practice in your country and the impacts on young people's human rights? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

- Parents and guardians lack digital-literacy and in most cases are unaware of the ill-effects of such exposure on mental and emotional well-being of children and young people.
- Young people become addicted to online games, videos,
- Lack of a comprehensive law governing the data privacy of citizens
    - Due to poverty, many young people have no access to digital devices
    - Young people from remote areas have least access to digital education due to lack od internet connectivity
    - Many Indian villages are still without electricity facility
    - Many young people are not aware of the importance of digital education
    - Many Schools and Colleges are without digital devices

5) What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.

Please provide any relevant statistical or disaggregated data based on age, gender, disability, ethnicity, religion, sexual orientation and gender identity, migration status, or other categories.

To regulate such activities that violate the rights of an Internet user, the Indian government has the Information Technology Act, 2000, in place. Here are some of its sections that empower Internet users and attempt to safeguard the cyberspace.

Section 65 – Tampering with computer Source Documents

A person who intentionally conceals, destroys or alters any computer source code (such as programmes, computer commands, design and layout), when it is required to be maintained by law commits an offence and can be punished with 3 years' imprisonment or a fine of 2 Lakhs INR or both

Section 66 - Using password of another person

If a person fraudulently uses the password, digital signature or other unique identification of another person, he/she can face imprisonment up to 3 years or/and a fine of 1 Lakh INR.

Section 66D - Cheating Using computer resource

If a person cheats someone using a computer resource or a communication device, he/she could face imprisonment up to 3 years or/and fine up to 1 Lakh INR

Section 66E - Publishing private Images of Others

If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge, the person is entitled to imprisonment up to 3 years of fine up to 2 Lakhs INR or both

Section 66F - Acts of cyber Terrorism

A person can face life imprisonment if he/she denies an authorized person the access to the computer resource or attempts to penetrate/access a computer resource without authorization, with an aim to threaten the unity, integrity, security or sovereignty of the nation. This is a non-bailable offence.

Section 67 - Publishing Child Porn or predating children online

If a person captures, publishes or transmits images of a child in a sexually explicit act or induces anyone under the age of 18 into a sexual act, then the person can face imprisonment up to 7 years or fine up to 10 lakhs INR or both

Section 69 - Govt.'s Power to block websites

If the government feel it necessary in the interest of sovereignty and integrity of India, it can intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. The power is subject to compliance of procedure. Under section 69A, the central government can also block any information from public access.

Section 43A - Data protection at Corporate level

If a body corporate is negligent in implementing reasonable security practices which causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages to the affection person.

As per Ministry of Home Affairs (MHA), to strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner, the Ministry of Home Affairs has provided financial assistance to all the States & UTs under Cyber Crime Prevention against Women & Children (CCPWC) scheme to support their efforts for setting up of cyber forensic-cum-training laboratories, training, and hiring of junior cyber consultants. Cyber forensic-cum-training laboratories have been commissioned in 28 States. The Central Government has taken steps for spreading awareness about cyber crimes, issuance of alerts/ advisories, capacity building/ training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensic facilities etc.

The Government has established Indian Cyber Crime Coordination Centre (I4C) to provide a framework and eco-system for LEAs to deal with the cyber crimes in a comprehensive and coordinated manner. 'Joint Cyber Coordination Teams' have been constituted for seven regions at Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam and Guwahati under the I4C to address the issue of jurisdictional complexity, based upon cyber crime hotspots/ areas, by on-boarding all the States/UTs to provide a robust coordination framework to the LEAs.

The Government has launched the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) to enable public to report incidents pertaining to all types of cyber crimes, with a special focus on cyber crimes against women and children. A toll-free number 1930 has been operationalized to get assistance in lodging online cyber complaints. The Citizen Financial Cyber Fraud Reporting and Management System module has also been launched for immediate reporting of financial frauds and to stop siphoning off fund by the fraudsters.

4. Details of the respondent

Respondent profile: Educator
Gender: Female
Country: India

Organization: IIMA India

1) What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

Many marginalized and vulnerable young people may not have access to the necessary digital devices, such as laptops, tablets, or smartphones. Inadequate internet connectivity, particularly in rural or economically disadvantaged areas, can impede access to online learning resources.

Some marginalized individuals may not be familiar with digital tools or lack the skills required for online learning. This can create a significant barrier to accessing and benefiting from digital education. Online education materials may not always be available in the languages spoken by marginalized communities, leading to difficulties in comprehension and effective learning.

2) **What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of specific laws and regulations, measures, policies, and programmes directed at ensuring young people's universal access to digital education.**

The Ministry of Education in India has undertaken many initiatives to promote digital education. Here are some key initiatives:

SWAYAM (Study Webs of Active Learning for Young Aspiring Minds)

It is an online platform offering free courses from elementary to postgraduate levels. It provides access to high-quality study material, video lectures, and interactive quizzes.

National Digital Library (NDL)

The NDL is a digital repository of educational resources. This includes textbooks, articles, audiobooks, videos, and lectures. It offers a vast collection of learning materials for students and teachers.

e-Pathshala

e-Pathshala is an online portal and mobile app. It provides access to textbooks, audio, video, and multimedia educational content. Content is available for school students from Class 1 to Class 12 in many languages.

DIKSHA

DIKSHA is a national digital platform. It hosts e-learning content for school students, teachers, and parents. It offers interactive lessons, worksheets, and assessments aligned with the school curriculum.

National Repository of Open Educational Resources (NROER)

NROER is a digital platform that curates and shares open educational resources. It provides a wide range of digital content. This includes textbooks, lesson plans, multimedia materials, and teaching aids.

Virtual Labs

The Virtual Labs initiative aims to provide remote access to labs for students and researchers. It offers a simulated learning environment. The users can perform experiments and gain practical knowledge.

National Programme on Technology Enhanced Learning (NPTEL)

NPTEL provides online courses and study materials in various disciplines. This includes engineering, science, humanities, and management. It is a joint initiative of the Ministry of Education and IITs.

Pragyatah

Pragyatah is a set of guidelines developed by the MoE to help schools use digital technology. The guidelines cover a range of topics. This includes the use of technology for teaching and learning and the management of digital resources.

For the differently-abled

- **Sign Language Channel: A dedicated DTH channel with sign language is available for hearing-impaired students. It provides accessibility and supports their learning needs.**
- **Digitally Accessible Study Material:** The study material has been developed in Digitally Accessible Information System (DAISY) format. This can aid hearing and visually impaired students.

Radio Broadcasting

- **Activity-based Learning:** Radio broadcasts focus on activity-based learning methods. This interactive approach engages students and promotes effective learning.
- **Community Radio Stations:** 289 community radio stations are utilized for this purpose. They broadcast content related to the National Institute of Open Learning (NIOS) for grades 9 to 12. This enables students in remote areas to access educational content.
- **Remote Area Education:** Radio broadcasting is particularly beneficial for students residing in remote areas. This is especially for grades 5 to 1. It helps bridge the education gap. It provides learning opportunities to those with limited access to traditional education.
- **Shiksha Vani Podcast:** Shiksha Vani is a podcast by the Central Board for Secondary Education (CBSE). It is utilized by learners from grades 12 to 9. Shiksha

Vani offers over 430 audio content pieces. It covers all subjects from grades 1 to 12. It facilitates learning through audio-based resources.

3) What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?
No response.

4) What are the main gaps and challenges to young people's protection from online threats in law, policy, and practice in your country and the impacts on young people's human rights? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.
No response.

5**) What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.**
There is an act : The information Technology Act (Amendment 2008)
The Indian Penal Code also contains several sections related to cybercrime. Sections 406, 408, 420, and 468 of the IPC deal with offenses related to online fraud and cheating. Section 509 deals with offenses related to online harassment and stalking

5. Details of the respondent

Respondent profile: Educator
Gender: Female
Country: India
Organization: IIMA India

1) What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

- Many marginalized families cannot afford personal devices like laptops, tablets, or smartphones.
- Inadequate internet connectivity in rural and remote areas hampers the ability to access online educational resources.
- High data costs and limited financial resources may prevent marginalized youth from accessing online educational content
- Limited exposure to digital technology and lack of digital literacy skills are significant barriers, especially for older individuals in vulnerable situations.
- Gender biases may limit girls' access to digital education due to cultural norms or concerns about safety.
- Discrimination based on caste, religion, or ethnicity can affect the opportunities available to young people, influencing their access to quality digital education.

2) What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of

specific laws and regulations, measures, policies, and programmes directed at ensuring young people's universal access to digital education.

- Digital India Initiative: Launched in 2015, the Digital India campaign aims to transform India into a digitally empowered society
- National Education Policy (NEP) 2020: The NEP 2020 emphasizes the integration of technology in education
- BharatNet Project: This project aims to provide high-speed broadband connectivity to all gram panchayats.

3) What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?

- Collaboration with Tech Companies: Governments often collaborate with technology companies to develop tools and features that enhance online safety.
- Awareness Campaigns: Governments hold public awareness campaigns to educate young people and their parents about the potential risks and challenges of the online world.
- Enhancing cybersecurity measures to help in creating a safer online environment.

4) What are the main gaps and challenges to young people's protection from online threats in law, policy, and practice in your country and the impacts on young people's human rights? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

- Lack of Comprehensive Legislation specifically to address online threats and the protection of young people

- Limited Enforcement: Even when laws are in place, enforcement may be weak. This could be due to a lack of resources, expertise, or coordination among different law enforcement agencies.

- Cyber bullying and online harassment are significant challenges for young people. The rapid growth of social media and online communication platforms has exposed young individuals to various forms of online abuse.

5) What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.

- National Cyber Security Policy (2013): The Indian government formulated the National Cyber Security Policy to ensure a secure and resilient cyberspace environment.
- Protection of Children from Sexual Offences (POCSO) Act, 2012
- Digital Literacy Programs: The government has initiated various digital literacy programs to educate young people about safe online practices and potential threats.
- Cyber Crime Cells: Many states in India have established specialized cybercrime cells or units to investigate and address online offenses, including those affecting young people.

6. Details of the respondent

Respondent profile: Adolescent (12-17)
Gender: Female
Country: India
Organization: Sisters of Our Lady of the Missions (RNDM).

1) What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of Marginalized young people and those in vulnerable situations in your response.

- The main challenges is poverty where having digital device for a girl in the area is difficult due to parents are not afford to pay.
- Educational institutions unable to upgrade according to the development of technology
- Illiteracy of the parents

2) What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of specific laws and regulations, measures, policies, and programmes directed at ensuring young people's universal access to digital education.

- Include digital education as part of academic studies.
- Providing tablets for the students in the government colleges
- Online academic studies

3) What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?

- Human Rights Day celebration in the school and colleges
- Inclusion of Human Rights topic in the syllabus
- Cyber awareness program in the school and colleges

4) What are the main gaps and challenges to young people's protection from online threats in law, policy, and practice in your country and the impacts on young people's human rights? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

- **Legal Framework:** While India has laws like the Information Technology Act, 2000, and the Protection of Children from Sexual Offences (POCSO) Act, 2012, there's a lack of specific legislation addressing all facets of online threats faced by young people.
- **Enforcement and Implementation:** Even when laws exist, enforcement and implementation are often weak, leading to impunity for perpetrators. Law enforcement agencies may lack the necessary training, resources, and technical expertise to effectively investigate and prosecute online crimes against young people.
- **Digital Literacy and Awareness:** Many young people, especially those from marginalized backgrounds, lack sufficient digital literacy to recognize and respond to online threats.

- **Cultural and Social Norms:** Sociocultural norms often perpetuate victim-blaming attitudes, discouraging young people from reporting online threats due to fear of stigma or retaliation.
- **Support Services and Counselling:** There's a lack of accessible and youth-friendly support services and counselling specifically tailored to address the mental health and psychosocial needs of young people affected by online threats.

5) What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.

- National Cyber Security Policy:
- Cyber Crime Cells:
- Digital Literacy Programs:
- Collaboration with Industry:

7. Details of the respondent

Respondent profile: Educator
Gender: Female
Country: India
Organization: IIMA India

1) What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

It's important to note that the challenges can vary widely depending on the socio-economic, geographic, and cultural context. Here are some general challenges:

1. **Lack of Infrastructure:** In rural or economically disadvantaged areas, there may be inadequate digital infrastructure, including limited access to high-speed internet, electricity, and necessary devices like computers or tablets.
2. **Digital Illiteracy:** Many young people may not have the required digital literacy skills to navigate online platforms, use educational software, or engage in virtual classrooms. This is especially true for marginalized populations.
3. **Financial Constraints:** Some families may face financial challenges in affording digital devices and maintaining a stable internet connection. This disproportionately affects marginalized and vulnerable populations.
4. **Language and Cultural Barriers:** Educational content might not be available in the languages spoken by certain marginalized communities. Additionally, cultural differences may affect the suitability of digital education materials.
5. **Gender Disparities:** Gender-based inequalities may influence access to digital education. In some cases, girls may face cultural or societal barriers that limit their access to online learning opportunities.
6. **Disabilities and Special Needs:** Young people with disabilities may encounter barriers to accessing digital education if online platforms are not designed to accommodate their needs. This includes issues related to accessibility and adaptive technologies.

7. **Security and Privacy Concerns:** Some families may be hesitant to engage in digital education due to concerns about online security and privacy. This is particularly relevant in cases where sensitive personal information is involved.
8. **Limited Support Structures:** Young people in vulnerable situations, such as those without stable homes or adequate parental support, may lack the necessary structure to engage effectively in digital education.
9. **Mental Health Challenges:** Extended periods of online learning can lead to increased screen time and potential mental health challenges, especially for young people in vulnerable situations who may lack proper emotional support.
10. **Unequal Educational Opportunities:** Marginalized communities may already face disparities in traditional educational opportunities, and the shift to digital education could exacerbate these inequalities.

It's crucial for policymakers, educators, and community leaders to address these challenges through targeted interventions and inclusive policies to ensure that all young people, especially those in vulnerable situations, have equitable access to digital education. Specific challenges will depend on the unique circumstances of each country and community.

2) What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of specific laws and regulations, measures, policies, and programmes directed at ensuring young people's universal access to digital education.

As of my last knowledge update in January 2022, specific details regarding government actions may have changed. However, as of then, several countries had been implementing measures to ensure universal access to digital education for young people. Here are some general examples of the steps governments were taking:

1. Infrastructure Development:
Governments were investing in building and upgrading digital infrastructure, including widespread internet access and reliable electricity supply, to ensure that students in both urban and rural areas can access online educational resources.

2. Digital Literacy Programs:
Implementation of digital literacy programs aimed at students, teachers, and parents to ensure they have the necessary skills to navigate online platforms and utilize digital resources effectively.

3. Device Distribution:
Some governments were distributing digital devices such as laptops or tablets to students who may not have access to them at home. This helps bridge the digital divide and ensures that all students can participate in online learning.

4. Online Content Development:
Governments were working on developing and curating digital educational content that aligns with national curriculum standards. This includes interactive lessons, e-books, and multimedia resources.

5. Legal Frameworks:

Some countries have implemented or updated legal frameworks to ensure that digital education is recognized and regulated appropriately. This may involve laws related to online learning platforms, data privacy, and online security.

6. Financial Support:
Financial support programs were introduced to assist families with low incomes in acquiring the necessary digital tools for their children's education. This could involve subsidies for internet connectivity or discounts on educational software.

7. Partnerships with Private Sector:
Governments were collaborating with private companies to enhance digital education initiatives. This could involve partnerships with tech companies to provide discounted or free access to educational resources.

8. Teacher Training:
Training programs for teachers to effectively use digital tools in education. This ensures that educators can adapt to the changing educational landscape and deliver quality online instruction.

To get the most accurate and current information, it is recommended to check with relevant government education departments, ministries, or official publications for updates on the specific laws, regulations, measures, policies, and programs in place. Keep in mind that the situation may have evolved since my last update in January 2022.

3) **What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?**
Here are some common steps:

1. Legislation and Regulation:
Governments may enact laws and regulations specifically addressing online rights and safety for young people. These regulations can cover issues like online harassment, cyberbullying, and protection of privacy.

2. Educational Programs:
Governments often invest in educational programs to raise awareness among young people about their rights and responsibilities online. This includes promoting digital literacy, responsible internet use, and online safety practices.

3. Cybersecurity Measures:
Governments work on implementing cybersecurity measures to protect young people from online threats such as cyberbullying, hacking, and other malicious activities.

4. Collaboration with Tech Companies:
Governments collaborate with technology companies to create and enforce policies that safeguard the rights of young people online. This may involve setting age restrictions, content moderation, and reporting mechanisms for inappropriate content.

5. National Strategies and Policies:
Some governments develop national strategies or policies focused on ensuring a safe and inclusive online environment for young people. These documents may outline specific goals, actions, and timelines for achieving online safety objectives.

6. International Cooperation:
Collaboration with international organizations and other countries helps in sharing best practices, resources, and strategies to address global challenges related to online safety for young people.

7. Helplines and Support Services:
Governments may establish helplines and support services that provide assistance to young people facing online threats or harassment. These services can offer counselling, legal advice, and other forms of support.

8. Privacy Protections:
Governments work to strengthen privacy laws and protections, ensuring that young people's personal information is handled responsibly and securely online.

9. Inclusive Internet Access:
Efforts to ensure that young people have access to the internet, promoting digital inclusion and reducing the digital divide, are also important for enabling them to exercise their online rights.

It's essential to stay informed about the latest developments in this area, as the digital landscape and policies are subject to change. Checking government websites, relevant international organizations, and news sources will provide the most up-to-date information on the steps being taken to protect young people's human rights online.

4) What are the main gaps and challenges to young people's protection from online threats in law, policy, and practice in your country and the impacts on young people's human rights? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.
1. Lack of Comprehensive Legislation: In many countries, there might be a lack of comprehensive and up-to-date legislation specifically addressing online threats and harassment, leaving young people without adequate legal protection.

2. Enforcement Challenges: Even when laws exist, enforcement can be a challenge. Law enforcement agencies may lack the resources or expertise to effectively combat online threats and cyberbullying.

3. Digital Literacy Gaps: Many young people, especially those in marginalized or vulnerable situations, may lack sufficient digital literacy skills to navigate online spaces safely. This can make them more susceptible to various online threats.

4. Privacy Concerns: The trade-off between online privacy and protection is a persistent challenge. Balancing the need to protect young people from online threats with the right to privacy requires nuanced legal frameworks.

5. Cyberbullying and Harassment: Cyberbullying is a significant concern, and policies may not be adequately addressing this issue. Marginalized young people may be more vulnerable to online harassment due to various factors such as discrimination or lack of support networks.

6. Access to Technology: Disparities in access to technology and the internet can exacerbate the vulnerability of marginalized young people. Limited access can restrict their ability to report threats or seek help.

7. Inadequate Support Systems: There may be a lack of support systems for victims of online threats. This is especially true for marginalized young people who may face additional barriers in accessing support services.

8. International Collaboration: As online threats often transcend national borders, effective international collaboration and coordination between countries are crucial. The absence of such collaboration can hinder efforts to address cross-border online threats.

9. Rapid Technological Changes: Laws and policies may struggle to keep pace with the rapid evolution of technology, making it challenging to address emerging online threats effectively.

10. Stigmatization and Discrimination: Marginalized young people may face stigmatization and discrimination online, impacting their mental health and overall well-being.

Addressing these gaps requires a multi-stakeholder approach involving governments, law enforcement, educational institutions, tech companies, and civil society to develop comprehensive and inclusive strategies for protecting young people online while respecting their human rights.

5) What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:

- These rules impose certain obligations on social media intermediaries to ensure the safety and security of users, particularly minors.
- Platforms are required to implement mechanisms to identify and remove explicit content involving children.

POCSO Act (Protection of Children from Sexual Offences):

- The Indian government has been actively using the POCSO Act to address online sexual exploitation of children.
- The act includes provisions to deal with the creation, transmission, and distribution of child pornography.

National Cyber Crime Reporting Portal:

- The government has set up an online portal to report cybercrimes, including those that target children.
- This portal facilitates the reporting of various cyber offenses, enabling law enforcement agencies to take appropriate action.

Digital Literacy Programs:

- The government has initiated digital literacy programs aimed at educating young people about online threats and safe internet practices.
- These programs often include awareness campaigns in schools and communities to educate children and parents alike.

Educational Initiatives:

- Integration of cybersecurity and digital literacy in the school curriculum to equip students with the knowledge to navigate the online world safely.

Child Online Protection Guidelines:

- The Ministry of Women and Child Development has released guidelines for child online protection, emphasizing the need for parents, educators, and platforms to work together.

Social Media Guidelines for Minors:

- Encouraging social media platforms to implement measures to protect minors, such as age verification mechanisms and parental controls.

It's important to stay updated with the latest information, as the government may introduce new policies and regulations to address emerging online threats. Always refer to the official government sources or announcements for the most recent developments.

8. Details of the respondent

Respondent profile: Educator
Gender: Female
On behalf of: Educators
Country: India
Organization: IIMA India

1) **What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.**

Although digital education has important strengths and provides unique access to quality education, the use of this platform has limitations that can pose potential challenges to the success of any online courses.

Computer Literacy: To work effectively in an online environment, both students and intermediaries must possess a basic level of computer literacy. They cannot excel in an online program if they do not have these technological tools

Lack of Teacher-Student Physical Interaction: How much teacher contact learners get on a physical campus is easy to underestimate. Then there is the instruction time itself, with the question-and-answer in real-time. Then right before and after training, once hours, chance encounters in the corridor, there is an opportunity for discussion ... all possibilities that are not accessible for digital education

Need for Self-Discipline

Technological Difficulties: We prefer to take it for granted that a laptop or desktop computer of the latest model is available to everyone. Not every student has had the same

access to technology. For all their online operation, many rely on their smartphone or a tablet.

Poor Time Management: This challenge is connected to the aspect of self-discipline, but it deserves its entry. One of the main benefits of this approach is that students can learn at their speed.

Transmitting virus: These programs attach themselves to a file and then circulate. They usually affect the data on a computer, either by altering or deleting

In India poor young people face lot of stress and constraints in accessing good digital education due to financial problems. There is lack of awareness about digital education which is a barrier to providing it to all. There is disparity between the rural and urban areas in providing digital education. Hence all the youth are not able to access it. Infrastructural problems, at times lack of motivation among youth, Lack of discipline, technical issues and course structure and quality not attractive to youth.

2) **What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of specific laws and regulations, measures, policies, and programmes directed at ensuring young people's universal access to digital education.**

Government has taken some measures which once again are not easily available to poor youth. Yes in schools computer education is introduced and compulsory all the students have to attend classes but the computers are not maintained well. Same in the colleges computer classes are held but not in good condition. At times teachers are not well trained. There are many rules and policies. Below are some of them.

- SWAYAM (Study Webs of Active Learning for Young Aspiring minds)
- National Digital Library (NDL)
- E-Pathshala
- DIKSHA (Digital Infrastructure for Knowledge Sharing)
- National Repository of Open Educational Resources (NROER)
- Virtual Labs
- National Program on Technology Enhanced Learning (NPTEL)
- The National Digital Literacy Mission (NDLM) which aims to train 500 million Indians in digital literacy by
- VidyaDaan,
- E-textbooks,
- PRAGYATA,
- Shiksha Vani,

3) What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?

- National Youth Policy which outlines actions that will empower the youth and ensure their safety and strengthen the legal system
- Bridging the digital divide for girls in India
- Child and youth safety online
- Engaging young people in open government
- The human based approach- focuses on those who are most marginalized excluded and discriminated
- Involving youth in positive youth development

4) **What are the main gaps and challenges to young people's protection from online threats in law, policy, and practice in your country and the impacts on young people's human rights? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.**

Young people especially the marginalized young are unaware of the protection policy in a digital world. For them just for fun and hobby to use mobiles and other media. They are not even aware of online safety. Only when they get into trouble then they realize how important to know about safety measures. Hence now all youth and children are spoken and sessions are organized by NGO's and colleges about cyber safety.

The marginalized youth in our project in the shelter homes and in the slums are very vulnerable and often become the victims of online threats and other forms of violence in the digital world.

5) **What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.**

The Central Government has taken steps for spreading awareness about cyber crimes, issuance of alerts/ advisories, capacity building/ training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensic facilities etc.

Central Government has taken steps to spread awareness about cyber crimes, issue of alerts/advisories, capacity building/training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensics facilities etc. to prevent such crimes and to speed up investigation. The Government has launched the online cybercrime reporting portal, www.cybercrime.gov.in to enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content. The Central Government has rolled out a scheme for establishment of Indian Cyber Crime Coordination Centre (I4C) to handle issues related to cybercrime in the country in a comprehensive and coordinated manner.

'Police' and 'Public Order' are State subjects as per the Constitution of India. States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes through their law enforcement machinery. The Law Enforcement Agencies take legal action as per provisions of law against the cyber crime offenders.

Further, Government has taken several steps to prevent and mitigate cyber security incidents. These include:

(i) Establishment of National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.

(ii) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.

(iii) Cyber Swachhata Kendra (Botnet Cleaning and Malware Analysis Centre) has been launched for providing detection of malicious programmes and free tools to remove such programmes.

(iv) Issue of alerts and advisories regarding cyber threats and counter-measures by CERT-In.

(v) Issue of guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

(vi) Provision for audit of the government websites and applications prior to their hosting, and thereafter at regular intervals.

(vii) Empanelment of security auditing organisations to support and audit implementation of Information Security Best Practices.

(viii) Formulation of Crisis Management Plan for countering cyber attacks and cyber terrorism.

(ix) Conducting cyber security mock drills and exercises regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.

(x) Conducting regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.

9. Details of the respondent

Respondent profile: Educator
Gender: Female
Country: India
Organization: IIMA India

1**) What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.**
Res: In a poor family, where the access may or may not be for mobile the online education or access to information is very difficult. Secondly, the average income of a parent doesn't permit the children to have access to digital education. Thirdly, network availability also a concern. Parents do doubt children if they use mobile.

2) What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of specific laws and regulations, measures, policies, and programmes directed at ensuring young people's universal access to digital education.
Res: Government has a separate Ministry of electronics and Information
Digital Personal Data Protection Act 2023
Information Technology Act 2000(IT Act 2000) and its Amendment
Cyber laws and policies

3) What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?

Res: The abovementioned laws have given the ways to report, communicate to the Government in Cyber branch and in the police department there is a department which can look into the cyber crimes reports of the students.

4) What are the main gaps and challenges to young people's protection from online threats in law, policy, and practice in your country and the impacts on young people's human rights? Please consider the specific situation of Marginalized young people and those in vulnerable situations in your response.
Res: The children are unaware of the danger of the social media and they are easily lured by the fake promises of friends, neighbours and known people. Many children are groomed online and they are vulnerable to this situation. They lose their human dignity.

5) What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.
Cyber laws
Digital Personal Data Protection Act 2023

10.Details of the respondent

Respondent profile: Educator
Gender: Female
On behalf of a group.
Country: India
Organization: IIMA India

1) What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

- There isn't sufficient electricity particularly in rural areas.
- Lack of proper study environment due to small houses with more members.
- Slow internet speed in most of the rural areas and also in some cities.
- Lack of sufficient devices for digital education.
- Lack of teachers who are expert in their subjects as well as in digital media

2) What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of specific laws and regulations, measures, policies, and programmes directed at ensuring young people's universal access to digital education.

- PM E-Vidhya: A comprehensive programme announced on 17th May 2020 with the objective to unify digital education with the education programs for better reach and access to E-learning. It targeted almost 25 crore students across the country.
- DIKSHA (Digital Infrastructure for Knowledge Sharing): It was initiated in 2017 with the dream of 'One nation, one digital platform'. It is a national platform for grades 1 to 12 and can be operated through a web portal or mobile app. It includes e-content respective to the curriculum with the assignments and courses for educators as well.

- SWAYAM Prabha TV: It has 32 channels for digital education with the objective of 'One class, one channel'.
- Vidya daan: Lauched in April 2020, with the objective to seek donations for digital educational resouces.
- E Pathshala: This initiatives focuses on teachers, parents as well as on students. It can be accessed through a web portal or mobile app.

3) What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?

1. The Indian Computer Emergency Response Team (CERT-In) which operates as the national agency to address the country's cyber security and has helped reduce the rate of cyber attacks on government networks.
2. Cyber Surakshit Bharat which aims at strengthening the cyber security ecosystem in India and follow the Government's vision of a "digital India.
3. Appointment of Chief Information Security Officers (CISOs) to identify and document the security requirements that may arise with each technical innovation.
4. Personal Data Protection Bill to protect Indian users from global breaches.
5. National cyber security policy 2013 to create safe and resilient cyberspace for the citizens.

4) What are the main gaps and challenges to young people's protection from online threats in law, policy, and practice in your country and the impacts on young people's human rights? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

- Some of the gaps and challenges are:
- Lack of transparency on sharing information
- The policies do not have sufficient measures on safeguarding the privacy of citizens
- Lack of awareness on the part of the youth regarding online threats
- Impact on their human rights: Violation of their right to freedom and privacy

5) What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.

IT Act 2000: Under this Act, sections 66 A, 66 C, 66 D, and 66 E, punishment is given to the person involved in any crime of insulting or fraud or privacy violation, etc., utilizing the internet, social media, and other digital media devices.

The Indian penal code 1860: The (IPC)Footnote7 is the official criminal code of India that covers all substantive aspects of criminal law, which came into existence in the year 1862 in all British Presidencies. IPC Sections 292A, 354 A, 354 D, 499, 507, and 509 punish people who indulge in blackmailing, harassment, stalking, threatening, intruding, etc.

POCSO ACT, 2012: Protection of children from sexual offenses (POCSO) is a complete law for protecting children below 18 years from the heinous acts of sexual assault, sexual harassment, and pornography.

The Nirbhaya funds scheme:

It is an initiative of the Government of India under the Nirbhaya funds scheme for ensuring the safety of women and children. The ministry of Home affairs generated a single number (112) Footnote 8 which was under the Emergency response support system (ERSS), to cope with any emergencies where immediate assistance from police, fire, and rescue, or any other help is required.

Cybercrime prevention against women and children scheme (CCPWC Scheme): Under the CCPWA scheme, different units are established that are responsible for reporting online criminal acts and their investigations, analysing cybercrime reports, and detecting any alarming cybercrime situation.
Indian cybercrime coordination centre (I4C) scheme: I4C acts as an essential tool to fight against cybercrime.

Please provide any relevant statistical or disaggregated data based on age, gender, disability, ethnicity, religion, sexual orientation and gender identity, migration status, or other categories.

- 50,035 cases of cybercrime were reported in India in the year 2020.
- Among which 1614 cases of cyberstalking, 762 cases of cyber blackmailing, 84 cases of defamation, 247 cases of fake profiles, and 838 cases of fake news were investigated.
- NCRB data Footnote1 reported that cybercrimes in India increased by 63.48% (27248 cases to 44548 cases) from 2018 to 2019, which upsurged by 12.32% in 2020 (44548 cases to 50035cases).