BASELINE STUDY AND POLICY GAP MAPPING REPORT ON 'ONLINE SAFETY FOR CHILDREN' IN BANGLADESH

Outreach Partner: team engine

Research Partner: Inspira Advisory & Consulting

unicef | for every child

BASELINE STUDY AND POLICY GAP MAPPING REPORT ON 'ONLINE SAFETY FOR CHILDREN' IN BANGLADESH

Outreach Partner: team engine

Research Partner: Inspira Advisory & Consulting

unicef | for every child

Credits:

Visualized Summary

HOW SAFE ARE OUR CHILDREN ONLINE?

A UNICEF research on Bangladeshi internet users

VICTIM OF CYBER BULLYING

EXPOSURE TO INAPPROPRIATE SEXUAL CONTENTS

40% BOYS

24% GIRLS

19% Children receive sextually inappropriate texts

12% Children get sextual images

5% Children are asked to send sextual images

RISKY ONLINE BEHAVIOUR

57% children befriend unknown people online

14% children meet online acquaintances

11% children share private information

ONLINE SAFETY SKILLS OF CHILDREN

SKILL DEFICIENCY HIGHEST AMONG MADRASAH STUDENTS

65% can block messages

44% have privacy settings knowledge

38% can block pop-ups

PARENTAL MONITORING

32% Boys never monitored

24% Girls never monitored

UNSUPERVISED INTERNET USAGE IS COMMON, HOWEVER.

USAGE & BEHAVIOUR PATTERN

63% children use internet at own room

49% children use parent smartphones

37% children use personal smartphones

INTERNET USAGE BY CHILDREN

94% own a social media account

42% use internet everyday

33% use internet for chatting

Source: Research Findings of Online Safety for Children in Bangladesh

A research on 1,281 internet user students between 10-17 years of age from 239 institutions in Bangladesh

Table of Contents

Executive

Executive Summary

Summary

Executive Summary

The internet population of Bangladesh has increased by 800 times since year 2000[1]. About 1 out of every 4 Facebook users in Bangladesh is a teenager (estimation based on Facebook API data). Children's online safety is a major concern worldwide, however, very few studies have been conducted in Bangladesh to investigate the online risks for children. The current study has two blocks;

a. Baseline survey on children's knowledge, behavior, perception and also their exposure to various online risks and harms.

b. Policy Gap Mapping.

Baseline Survey:

The baseline survey was conducted on school-going children (aged 10 to 17) who use internet. A total of 1281 students (653 boys and 628 girls) from 239 educational institutions (school, college, madrasah) were surveyed.

Key Findings:

Usage and behavioural pattern

About 25% of the children (aged 10-17) started to access the digital world below the age of 11. A large majority (63%) of the children use their own room as the primary internet usage point. This indicates the prevalence of "bedroom culture" which allows for more personal and less supervised internet use. Smartphone is the most used device for using internet: 49% of children use their parents' smartphone and 37% of children use their own smartphone.

Some 42% of respondents use internet every day though the frequency of internet access varies across different groups of children. The gender difference

[1] Study: Internet users in Bangladesh have increased 800x since 2000, *Dhaka Tribune. Retrieved from https://www.dhakatribune.com/bangladesh/2018/10/23/internet-usage-increasing-across-asia*

is noticeable; boys (63%) are ahead of girls (48%) in terms of high frequency access[2]. About 94% children from English medium background use internet every day. In contrast, children from Bangla medium schools and Madrasahs are less frequent users. Chatting online and watching video are the two most frequent internet activities; 33% chat online every day, and 30% watch video every day. Boys perform all forms of online activities more than the girls do. For majority of the online activities, daily engagement is higher among urban and older group (16-17)[3] of children.

Online safety skills

The research attempted to assess children's online safety skills in four key areas; ability to change privacy settings in the social networking site/app they use, ability to block message of unwanted person, ability to use 'report' option for unwanted content/fake account, and ability to block pop-up ads. Skill deficiency was high for all four online safety skills. Twenty-six per cent (26%) of the respondents have none of the four safety skills explored in the study.

Some 65% of the respondents know how to block message, 45% can change privacy setting, and 42% can use 'report' option, and 38% can block pop-up ads.

Furthermore, skill deficiency is highest among the rural children of Bangladesh. Comparison based on medium of schooling shows that skill deficiency is highest among Madrasah students.

Risky online behavior

The study investigated different risky online activities which fall under two broad categories: sharing of private information and content, and contacting with online acquaintances.[4]

A total of 10.8% children said that they shared their personal information with online acquaintances in one year preceding the study. Befriending unknown person in the internet is a common form of risky online behavior among all children. Majority (57%) of the children admitted to befriended unknown people in the internet. Children also make various forms of offline contact after befriending a person in the internet. An astonishing number (14%) of children said that they had met with an online acquaintance face to face.

[2] Accessing internet 'every day' or '4-5 times a week' were considered 'high frequency accesses.

[3] Respondents were divided into three groups for comparative analysis: age group 10-13, age group 14-15, and age group 16-17.

[4] If a child got acquainted with a person in the internet, the person has been termed as an online acquaintance.

Some groups of children engage in riskier online behaviors than others do. For instance, rural children showed a greater tendency in all risky activities related to sharing of private information or content. As to age, the oldest group of children (16-17) engaged in all forms of risky behaviors more than younger groups of children. Another risky behavior explored in the study was password sharing. Some 10% of the respondents stated that they had shared password with someone other than family members.

Exposure to sexually inappropriate content

Some 19% of the participants stated that they had received sexually inappropriate text, and 12% had received sexual image or video one year preceding the study. Five per cent (5%) of the respondents stated that they had been asked or insisted by someone to send their own nude or seminude image or video. Children of Khulna division are more exposed with regard to receiving sexually inappropriate text or content (image/video). Percentage of children who admitted being asked or insisted to send their own nude/semi-nude image or video was highest in Khulna.

Online harms

Among different online harms explored in the study, virus attack is the most common form of harm with some 37% of the respondents saying that their devices got infected with virus. Some 32% said that they were bullied online. Children reported being bullied for their appearance, exam result, religion etc. Other major harms are; account hacking 16%) and fake account (13%).

Experience of online harms varies across different groups of children. Children aged 16 to 17 experienced all forms of online harms more than younger groups of children. Area wise differences are visible as well; urban children in general are exposed online harms more than peri-urban and rural children. As to sex, boys experienced majority of the online harms more than girls did. The gender difference was biggest in the experience of online bullying. Forty per cent of the (40%) of the boys experienced at least one form of cyber bullying, whereas for girls the figure was 24%.

As to division, 40% of the children in Khulna reported cyber bullying, a figure that is higher than that of any other division.

The study also explored exposure to religious provocation, 10% of the children faced religiously provocative content. Boys and older children (16 to 17) have been exposed to such provocative content more than other groups of children.

Policy Gap Mapping

Following laws and policies were reviewed:

- Information and Communication Technologies Act 2006
- Pornography Control Act (2012)
- Digital Security Act (2018)
- National ICT Policy of Bangladesh 2018
- National Education Policy of Bangladesh 2010

The gap mapping analysis reviewed the abovementioned laws and policies in accordance with the rights-based approach of *United Nations Convention on the Rights of the Child* and explored the loopholes of those Bangladeshi laws and policies which are contrary to it.

Int

1.0

Introduction

troduction

1.0 Introduction

1.1 Context

The internet population of Bangladesh has increased by 800 times since year 2001)[5]. According to Bangladesh Telecommunication Regulatory Commission, the industry has added 1.44 crore active connections in one year alone (July 17 to June 18)[6]. There has been a national drive towards digitization in Bangladesh, and the recent introduction of fourth-generation (4G) mobile internet in the country is likely to increase internet usage even more.

With the increasing internet penetration in the country, children are also getting more involved in the virtual world. Although there exist little data about child internet-users in Bangladesh, data on Facebook users provides a glimpse about how large the number could be. About 1 out of every 4 Facebook users in Bangladesh is a teenager (estimation based on Facebook API data). While the virtual world offers infinite opportunities, it has dark side as well. There has been increasingly growing concerns across the world about new dimensions of threats like cyberbullying, online sexual abuse, online sexual exploitation, cyber radicalization, online attacks and frauds and online enticement which have negative consequences in offline too. Internet being a self-usage tool; users themselves are primarily accountable for their personal safety. However, in case of children and teens, the *risk burden falls on* caregivers, educators, government agencies, the internet ecosystem players.

Considering this surge of internet & digital adoption, IT education has been made compulsory at secondary level in 2013 with the plan to expand that to primary level by 2021. However current IT education curriculum has more focus on technical training and less on internet safety, and ethical and social use of

[5] Study: Internet users in Bangladesh have increased 800x since 2000, *Dhaka Tribune. Retrieved from https://www.dhakatribune.com/bangladesh/2018/10/23/internet-usage-increasing-across-asia*

[6] Islam, M., Z. (2018, August 20). Mobile data leads to internet boom. *The Daily Star. Retrieved from https://www.thedailystar.net/news/business/telecom/mobile-data-service-leads-to-internet-boom-in-bangladesh-1623310*

ICT. There is a general dearth of **strategically disseminated internet safety awareness contents/campaign** in the country, leading to a poor state of internet hygiene. The current study intents to fill the knowledge gap by exploring children's knowledge, behavior, perception, exposure to various online risks and harms, and also by mapping the loopholes in the existing legal/policy fabrics for future strategic interventions.

1.2 Project Design

The project focusing on filling the knowledge gap on online safety for children has two fundamental blocks; a baseline study on children's knowledge, behavior, and perception within the context of internet safety, and a gap mapping study on existing laws/policies that deal with or have the potential to deal with online safety issues.

Block: 1: Baseline Study

The broad goal of the baseline study was translated into three specific objectives:

Objectives

Understanding children's internet usage and behavioral patterns in Bangladesh.

Measuring children's level of awareness and skills related to internet safety.

Exploring risks, harm and vulnerabilities arising from internet usage of children.

Block: 2: Policy Gap Mapping

The Information and Communications Technology Act 2006, Digital Security Act 2018 and the Pornography Control Act 2012 are the main criminal laws to deal with online harassment against child in Bangladesh. Besides, National Information and Communication Technology Policy 2018 and the Education Policy 2010 are two key policy frameworks that have the potential to deal with online safety of the children in Bangladesh. These laws and policies have been reviewed to identify gaps and to provide actionable recommendations.

1.3 Guiding Framework for the Project

Approaching the two key blocks of the project required a systematic approach, hence, a guiding framework was developed. The framework was inspired by the works of Livingstone, Mascheroni and Staksrud (2015). The original model provides an extensive framework in understanding the opportunities and risks children with different identities and resources face online, and how these affect their well-being. To fulfill the purpose of the current project in hand, only relevant components of the mentioned framework were adopted. For example, instead of digital skills component, this research limited the scope to skills related to online safety. Besides, all the components in the framework were not necessarily covered in both the baseline study and policy gap mapping.

The framework which has been utilized to conduct this research has been detailed below:

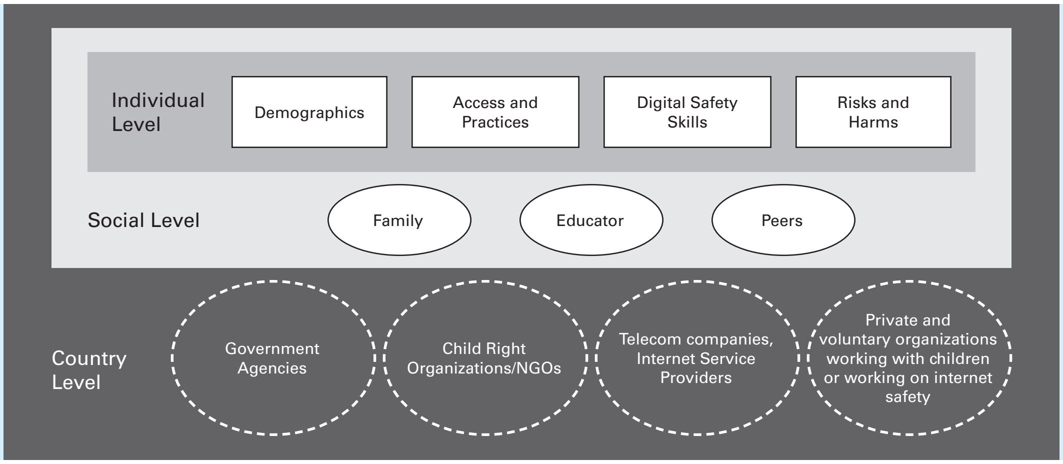

Individual Level
Demographics
Access and Practices
Digital Safety Skills
Risks and Harms
Social Level
Family
Educator
Peers
Country Level
Government Agencies
Child Right Organizations/NGOs
Telecom companies, Internet Service Providers
Private and voluntary organizations working with children or working on internet safety

Figure 1: Guiding framework: Inspired by the work of Livingstone, Mascheroni and Staksrud (2015).

Individual Level:

Demographics

Demographic factors considered in the study are; age, gender, and geography. These are some of the most important characteristics of a child's identity and these characteristics are likely to influence his/her internet behavior, knowledge and perception. Medium of schooling was also considered a key demographic factor in the study. Bangladesh has three major streams of education; Bangla medium, English medium and Madrasah. These three-schooling systems have different curricula, and teaching approach.

Access

This component looks into the diversity of internet access, covering place and device and frequency of access. Understanding how children access internet access is important as it influence their digital practices, opportunities and skills. Access is also important to understand children's vulnerability to risks and harms in the internet

Practices

This segment explores online activities performed by children in Bangladesh. Online practices include but not limited to activities in relation to learning, online communication, entertainment, personal and commercial use.

Online safety skills

This component looks into different online safety skills that help children to protect themselves from risks and harms in the internet.

Risks and harm

This segment explores children's exposure to risks and harm online, and their coping mechanism. The component relate to Content, Contact, and Conduct related risks that children are exposed to. This segment also attempts to understand actual harms arising from online risks and children's coping mechanism.

Social level:

Social level actors including parents/guardians, educators and peers influence children's online and offline behaviours. These actors are also important in creating awareness, imparting online skills and acting as support system when children face negative experiences online.

Country Level Actors:

The country level actors shape the internet ecosystem, create awareness, and provide the support system for children experiencing online risk or harms. Roles of country level actors were not covered in the baseline survey. These actors were reached out to understand their roles and perspectives within the context of the policy gap mapping study.

1.4 Structure of the Report

The report has been divided into two parts. First part of the report will present a brief literature review, methodologies, analysis and findings of the baseline study encompassing the knowledge, behavior and perception of children. The second part of the report will present the review of existing laws and policies in Bangladesh. This part will law out some recommendations with major focus on legal/policy reform, enactment, and implementation.

Base

2.0

Part 1: Baseline Study

line Study

2.0 Part 1: Baseline Study

2.1 Literature Review

Access and intensity of internet usage among Children

Children account for one out of three internet users around the world (UNICEF, 2017). Intensity of *internet use is high in the technologically advanced or industrialized world*, although low and middle-income countries are catching up rapidly. Generally, in richer countries and among better-off children in all nations, access to and usage of the internet are greater than the poorer countries and less well-off children (Uwe Hasebrink, 2011).

Around the world, children at very early ages are starting to access the digital world. A prior study on internet usage by Indian children shows a mean age to start using the internet is *10 years (±2.3)* (Govidnappa Lakshmana, 2018). A report published in the final quarter of 2017 on rural areas of Nepal tells that the starting age to use the internet is 14; some early adopters reported starting use at age 12. (PALO, 2018). A pilot study conducted in the Philippines on children aged 9 to 17 found that average age of first internet use was 9 years old (Tan, Estacio, & Ylade, 2016)

Miniaturization of devices are rapidly changing how and when children go online In the UK, more than half of the respondents (53%) go online in their own room, nearly the same amount (43%) on a games console and two-thirds (66%) also use their smartphone for internet access (McAfee, 2013). Study on Argentine children revealed 92% of the respondents use private spaces of their house, and *mobile phone is the device most used by children to surf the internet (89%)*, being considered the most practical and accessible. (GLOBAL KIDS ONLINE ARGENTINA, 2016). Hence, smartphone is fueling a 'Bedroom culture' allowing for *more personal, more reserved, and less supervised online experience* (UNICEF, 2017).

In an Indian study, *the maximum number of hours spent online by kids in India was over 8 hours a week for various purposes*. (Govidnappa Lakshmana, 2018). Study on Argentina children revealed that 51% use the internet all the time, 20%

did so more than once a day and 16% more than once an hour (GLOBAL KIDS ONLINE ARGENTINA, 2016). In South Africa, 39.8% of the respondents of a study reported that they use internet daily or almost every day (Phyfer, Burton, & Leoschut, 2016)

Children go online for many reasons, and these change over time, shifting broadly from engaging with mass-produced content to also engaging with online communication. Childwise's Monitor Report 2017 found that children aged 7-16 use the internet to do the followings (Professor Sonia Livingstone, 2017):

- Watch video clips (59%),
- Listen to music (56%),
- Play games (54%),
- Complete homework (47%),
- Interact with family and friends (47%),
- Social networking (40%),
- Look up information (38%),
- Upload videos, photos and music (27%).

As children get older, music and communication become more important while playing games declines.

Risk, Harm and Vulnerability

While children are exposed to a wide range of risks online, not all risks result in harm for children (UNICEF, 2011). *Actual harm resulting from risk could vary depending on the type of risk and country context* (Lobe, Livingstone, Olafsson, & Vodeb, 2011). Besides, some children could be in a more vulnerable situation than others.

Online risks can be classified into three broad categories: Content Risk, Contact Risk, and Conduct Risk (Livingstone, Haddon, Gorzig, & Olafsson, 2011)

- Content risks: This risk is related to inappropriate content, such as sexual image, violent image, hate speech etc. Child is the recipient of these contents.
- Contact risks: Children may intentionally or unintentionally engage in risky activities initiated by adults. For instance, sending nude images to adults is a contact risk.
- Conduct risk: Children can behave as an actor in creating content and contact risks for other children. For instance, bullying other children is a conduct risk.

Above mentioned risks with some examples are given in the table below:

	Content	Contact	Conduct
Aggressive	Violent / gory content	Harassment, stalking	Bullying, hostile peer activity
Sexual	Pornographic content	'Grooming', sexual abuse or exploitation	Sexual harassment, 'sexting'
Values	Racist / hateful content	Ideological persuasion	Potentially harmful user-generated content
Commercial	Embedded marketing	Personal data misuse	Gambling, copyright infringement

Figure 2: Typology of Risks with examples (Livingstone, Haddon, Gorzig, & Olafsson, 2011)

Risky Activities

Sharing private information online is one of the most common risky behaviors. Analyzing the social networking habits of Indian children and teenagers, McAfee study (2014) showed that *70% of the respondents shared their contact details such like email, home address online* (Financial Express, 2014). A study on school children of West Bangalore (India) found that 33% of respondents put their personal information on various Websites, and the majority of them were at risk of viewing sites with nudity and sexual images (Lakshmana, Kasi, & Rehmatulla, 2017). A cross country study on 25 European countries indicates that only 42% of the respondents maintain fully privacy of their social networking sites, 18% maintain partial privacy and 26% keep their profile fully public (Livingstone, Haddon, Gorzig, & Olafsson, 2011). A study on South Africa showed that around 21% of the child participants shared their video or photo, and 14% shared their personal information like address with people who they had never met in person (Phyfer, Burton, & Leoschut, 2016).

Studies on various countries show contact related risky activities by children. The McAfee study showed *53% of the Indian youth met someone who they only knew online* (Financial Express, 2014). A study in the context of child users in Europe found that around one-third of the respondents contacted with someone they never met face to face within one year preceding the study and 9% of the participants met with someone in person who they knew online (Livingstone, Haddon, Gorzig, & Olafsson, 2011).

Negative experiences and Harms

Cyberbullying includes “emotional harassment, defamation and social exposure, intimidation, social exclusion” (Singh & Bishnoi, 2016). According to the study by Microsoft (as cited by Singh & Bishnoi, 2016), almost half the children responding to the survey (India) experienced some negative online activities that could be termed as bullying. Around 29% said that someone called them by bad names, and 22% had undergone mean or unfriendly treatment. In a study on South African children, 22% of participants said they had been sent hurtful or nasty messages, and 14.9% claimed that nasty messages about them had been floated online (Phyfer, Burton, & Leoschut, 2016). Child sexual abuse can be defined as “a sexual activity between a child and an adult or another child who by age or development is in a relationship of responsibility, trust or power, for gratifying or satisfying the needs of the latter” (Singh & Bishnoi, 2016). Exposing children to online sexual content also falls under the child sexual abuse. According to the U.S based organization, The National Center for Missing and Exploited Children (NCMEC), over 2,446,884 cases of online sexual abuse were reported in India in 2017 alone. According to cybercrime expert, Guillermo G, “WhatsApp is the most common means by which pedophiles exchange images of children”. He also cited Facebook as a medium where sexual abusers are active (The New Indian Express, 2018).

Seeing sexual images is another common content related risk. EU kids Online survey found that 23% of the surveyed children had seen sexual images online or offline within one year preceding the study, and internet was one of the most source. There is variability in exposure to sexual images depending on ages. The study showed that 36% of children aged 15 to 16 had seen sexual images, while 11% of the 9-10 years such images (Livingstone, Haddon, Gorzig, & Olafsson, 2011). Study on Brazilian kids found that 26% of the participants reported having seen sexual images within one year before the study, and 44% among them saw these contents on internet (ICT Kids Online, 2012).

Children are not only exposed to seeing sexual content online, some children are also creating sexual content. User generated content such as “Sexting” is become common trend among many youths. Sexting is defined as “exchange of sexual messages or images”. There are a wide range of motivation for sexting, including innocent expression of sexuality and coercion. Research findings indicate that when self-generated sexual content were uploaded elsewhere online, up to 88% of the time no permission was taken from the creator of the content (UNODC, 2015).

Vulnerability to Harm

UNICEF reported that there have not been sufficient studies regarding children's online safety in some of the most disadvantaged communities[7]. However, existing studies show that females, children from lower social economic background, children in communities lacking knowledge in sexual abuse and exploitation of children, non-school going children, and children suffering from physical and psychological problems are most vulnerable (UNICEF, 2017) . Access and medium of internet can also affect children's vulnerability to many forms of harms. Accessing internet through cybercafé can expose children to various contact-related risks from adults (UNICEF, 2011). EU Kids Online survey showed that when parents had lower education and internet experience, children would lack digital safety skills and parental support. This made children more vulnerable. The same report showed that children having psychological issues faced more online risk than others (Livingstone, Haddon, Gorzig, & Olafsson, 2011). Some risky activities make children more vulnerable to harms than others. For instance, self-generated sexual content by the children make them more vulnerable to sexual abuse, exploitation and "revenge porn" (Singh & Bishnoi, 2016).

Roles of influencers

EU Kids Online developed a typology for mediating the internet (Uwe Hasebrink, 2011):

- Active mediation of a child's internet use comprises of talking with adolescents about specific media undertakings or sharing these activities with them. This mediation includes guiding children in online safety, either by assisting them when they are in trouble, or by telling them what to do in a displeasing or troubling situation.
- Restrictive mediation includes setting up guidelines regarding what children can or cannot do.
- Monitoring encompasses checking children's profiles on a social networking site or the mails in their email checking the computer to see what children have been doing or instant messaging account.
- Technical mediation commonly involves particular software built to filter as well as limit certain kinds of unwanted use.

  Norton Security, a firm dealing with online security and protection, found that awareness of risks among adult Indians was significantly lower than global levels of concern based on the "it won't happen to me" syndrome.

[7] Vulnerability indicates a set of contingencies that mediate the relationship between risk and harm.

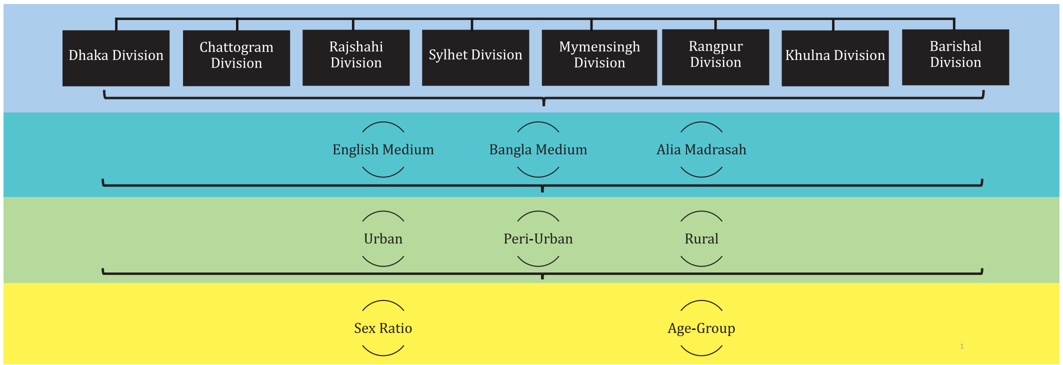
The same misplaced confidence probably extends to the risks faced by children online. About 60% of the parents across 8 metro areas in India shared that their adolescents had consulted them regarding things that disturbed them online (UNICEF, 2016). According to the report by McAfee, in India, a mere 36% parents said they used software to monitor their children's activity on these devices (The Economic Times, 2017).

In many cases, *kids are more technologically progressive than grownups*, so some parents feel intimidated and abstain from enforcing rules that are imperative to protect their children as they surf and socialize online. (UNICEF, 2011).

2.2 Methodology

Sampling Distribution

The population of the study are Bangladeshi children aged between 10 and 17, who use internet and are enrolled in mainstream education system. Selection of the study population was based on project priorities, future intervention plans and a pre-research survey. A total of 1281 children from 239 educational institutions were administered the questionnaire survey. To ensure proportionate participation, firstly, the sample was distributed throughout national administrative zone based on enrollment rate in different medium of education[8]. Next, the sample size was distributed into different geographic spread (e.g. Urban, Peri-Urban, Rural)[9] based on national education statistics. For other demographic characteristics like age and gender, researchers used gender and age wise enrollment.



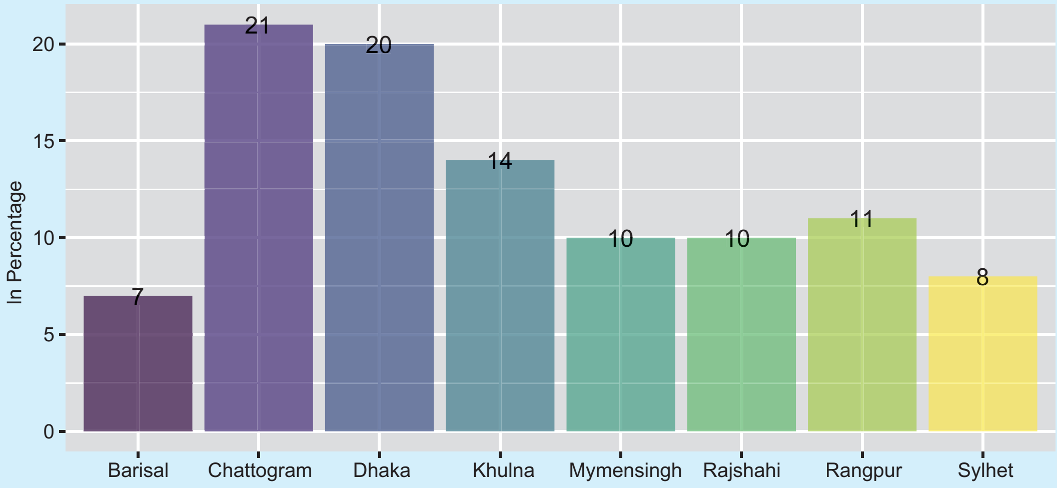
[8] Medium Schooling: English Medium, Bangla Medium and Alia Madrasah. Qawmi Madrasah was excluded from the study.

[9] Divisional cities were classified as urban areas; Major cities at the district level were categorized as Per-urban areas and the rest were termed rural areas.

Sample Characteristics

Geography

The figure below shows the distribution of the respondents across eight divisions[10] in Bangladesh.



Barisal	Chattogram	Dhaka	Khulna	Mymensingh	Rajshahi	Rangpur	Sylhet
87	264	254	173	130	130	138	105

Figure 3: Respondents by divisions

The survey sample constituted 434 respondents (34%) from urban areas, 397 (31%) respondents from peri-urban areas and 450 respondents (35%) are from rural areas.

Sex of the Respondents

In total, 653 respondents (51%) were male and 628 respondents (49%) were female. This ratio closely resembles that of gender wise participation ratio at primary, secondary and higher secondary level in Bangladesh.

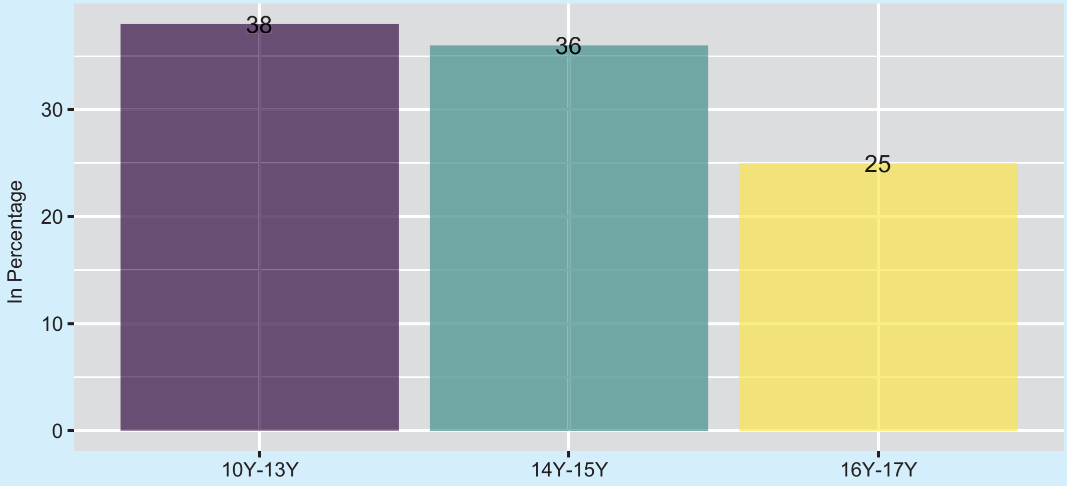
Medium of Schooling

About 81% the respondents were from Bangla medium institutions, 5% were from English medium institutions and 14% were from Madrasahs. The ratio resembles the national enrollment numbers at three streams of education system in Bangladesh.

[10] Bangladesh is divided into eight major administrative regions called division

Age of the Respondents

The figure below shows that 38% of respondents are aged between 10 to 13 years, 36% of respondents are aged between 14 to 15 years and 25% of respondents are aged between 16 to 17 years. The reason behind smaller ratio of the children aged 16-17 is due to lower enrollment number at Higher Secondary level.



10 to 13 years	14 to 15 years	16 to 17 years
493	466	332

Figure 4: Age of the respondents

Scope and Instruments

The guiding framework as explained in the first chapter has many components, and each of these components themselves could be vast and sometimes multi-dimensional in nature. Therefore, it was important to limit the scope of each component to conduct meaningful investigation within the confines of different project constraints. The below table provides a glimpse of the topics explored in the study:

Access	Frequency of internet Access
	Device used for accessing internet
	Frequency of internet Access
	Social media account
	Age of first exposure to internet
Practices	Learning activity
	Reading News

	Communication (chatting, email)
	Entertainment activities (gaming, watching videos, listening to music).
	Social media activity
	Looking for information to buy/sell products online
Online Safety Skills	Ability to blocking message from unwanted people
	Ability to changing privacy setting in the social media
	Ability to use 'report option'
	Ability to block pop-up ads
Risky Online Behaviours	Sharing of private information and content
	Password sharing
	Befriending unknown people online
	Establishing contact with online acquaintance (over phone call, video call, or meeting in-person
Risk related to sexually inappropriate content	Receiving or sending/sharing sexually inappropriate text/image/video
	Being persuaded to send own nude/semi-nude image, video.
Other risk or harms	Security breach (hacking)
	Attack on device
	Cyber bullying
	Fake account
	Losing money by being cheated in the internet.
	Sharing of private information without consent
	Sharing of negative/false/inappropriate information
	Religiously provocative content
Coping mechanism	Help seeking behaviour
Mediation by parents/ guardians	Active mediation
	Restrictive mediation
	Monitoring

A pre-research survey conducted on around 100 school going children in Dhaka helped at the initial phase of the questionnaire development. The research instruments drew largely from the work of 'EU Kids Online' network funded by the EC (DG Information Society) Safer Internet Programme (project code

SIP-KEP-321803) (www.eukidsonline.net), Global Kids Online Research toolkit (www.globalkidsonline.net), and from other international publications. The questionnaire was reviewed and edited by a child psychologist to make it more child friendly. After developing the questionnaire, a pilot study was conducted on 40 students at two schools in Dhaka, and the questionnaire was finalized after further refinement.

The survey was conducted on November 2018. Steps followed in the survey process are:

a. Authorities of the educational institutions were contacted and requested for permission.
b. Upon permission, trained enumerators visited the institutions. They went to each classroom (class: 5-12), described the purpose of the research and randomly selected students who claimed to be internet users.
c. Students who were willing to take part in the survey were then brought into an empty classroom, where they filled up the survey questionnaire.

Along with the school-based survey, an online questionnaire was floated on Facebook of some media partners whose followers had good representation of the study population. The online channel constituted only a small proportion of the survey sample (around 10%).

Ethical Consideration

The research team did not seek ethical approval due to the absence of established practice of receiving ethics committee appraisal on social/behavioral research in Bangladesh. However, the team followed internationally recognized ethical framework. The study followed the key ethical issues specified in the method guide of the Global Kids Online[11].

Key Ethical issues:

Privacy: The research team anticipated that privacy from other children would be a key an issue since the survey was school-based. Hence, the selected respondents from different classrooms were taken to a separate room which allowed for sufficient distance among the respondents. The research team assumed that children might not feel comfortable in telling about their internet behavior in front of their teachers within the cultural context of Bangladesh. Therefore, teachers were requested not to stay in the class when children were asked whether they use internet, and when they were filling up the survey questionnaire.

[11] Bergman, G. (2016). Ethical considerations for research with children. London: Global Kids Online

Managing distress: Due to the sensitive nature of some questions, the survey questionnaire was reviewed by a child psychologist to ensure these questions do not cause any distress on children. The enumerators were properly trained to deliver the message that the respondents could discontinue any time that wanted.

Informed consent: Parents entrust school authorities to act as gatekeepers and to act as responsible adults working in the best interest of children. Since, it was a school-based survey, informed consent was taken from the representatives of school authorities (e.g. headmaster). However, even when the school authorities permitted the survey, they were generally reluctant to sign any document. Therefore, taking consent was done mainly over the phone, and over email and face-to-face communication. The field enumerators explained all the features of the research to the children. Children were given the liberty to participate or not to participate in the research, and their decision to discontinue participation at any time was respected.

Inclusion and exclusion: The research team reached out to geographically remote and socio-economically backward areas. Even with the best intention, the research team could not conduct survey on marginalized children (e.g. children with disabilities) or in areas with marginalized communities (e.g. indigenous communities) due to the project constraints.

Payment and compensation: No payment or compensation was made for participating in the survey.

Use of interpreters: Interpreters were not required for the survey since the research team knew the language of the participants. However, all enumerators were recruited locally so they knew local dialects.

2.3 Internet Usage and Behavioral Pattern

Internet usage and behavioral patterns illustrate how children are accessing internet and what activities they are performing. In line with the guiding framework, usage and behavior patterns have been translated into two parameters; access and practices. Access and practices are important to understand the overall context and environment within which children experience the digital world, and take up different online opportunities. This chapter, divided in two sections, will depict the diversity in access and practices among different groups of children in Bangladesh.

2.3.1 **Access**

Age of Internet Exposure

The respondents were asked at what age they used internet for the first time. The mean age of first exposure to internet was found 12.07 years. Some 25% of the respondents started accessing the digital world below the age of 11.

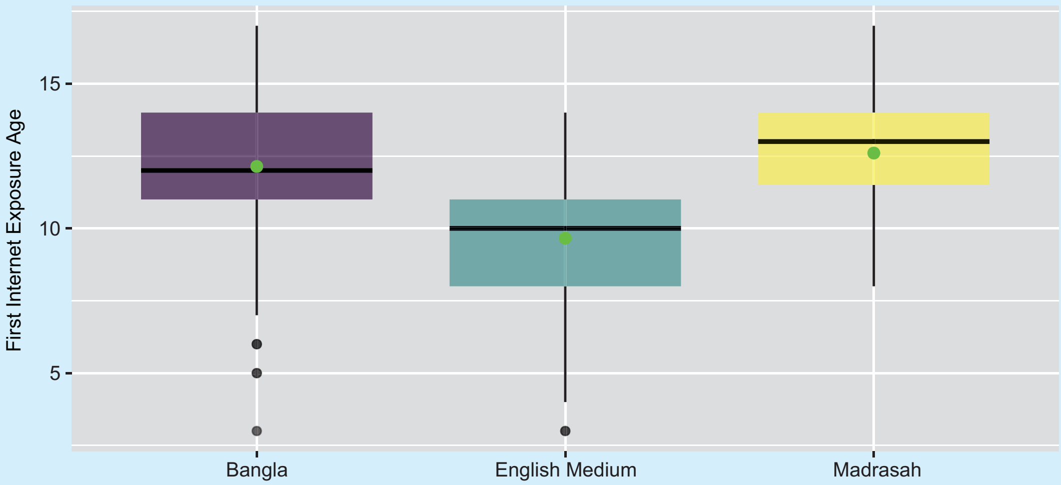


Figure 5: Age of exposure to internet by medium of education

Figure 5 indicates that students from English medium background started to use internet at the age 9.66, which is lower than that of Bangla medium (mean=12.13) and Madrasah students (12.6). Hence, it can be said that English medium get exposed to internet relatively earlier in their life than Bangla medium and Madrasah students.

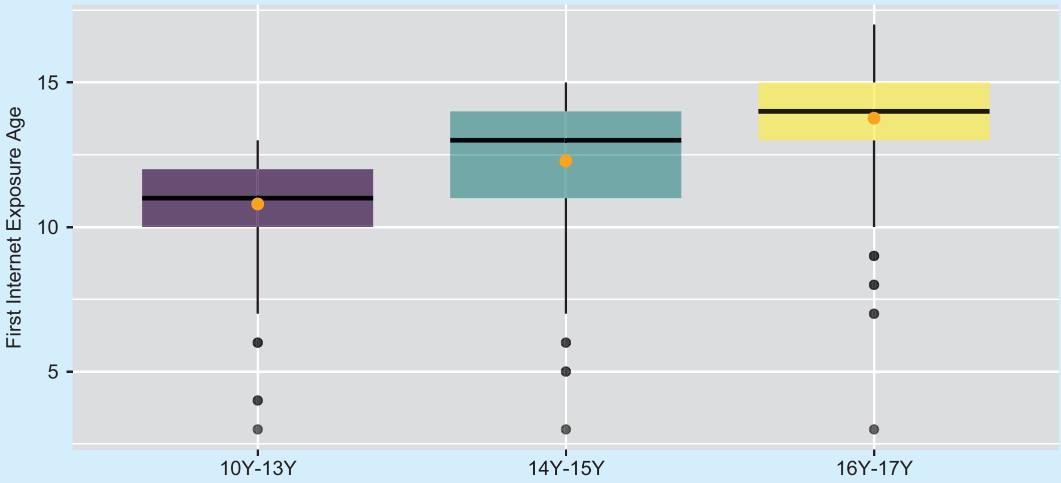


Figure 6: Age of exposure to internet by age group

Another interesting finding is that mean age of first exposure to internet goes up as we move from a lower age group to a higher age group (see the figure 6). This indicates that children are adopting internet at increasingly earlier ages.

Device and Place of Internet Access

Device and place of internet use are important to understand the scope of supervision and monitoring of children's internet activities. For instance, a child can use the internet completely unsupervised if the location is an internet café or any other private place. Similarly, if the device is owned by parents, there are more scope of parental control.

Place of Use

Home is the most used internet access point among children aged between 10 and 17. Figure 7 shows that 63% of the respondents use internet in their own room, and similar percentage also use common room (e.g. living, dining room). These figures highlight two contrasting situations. Since a significant number of children are using internet at the common room, this offers opportunities for parents and guardians to apply filtering, monitoring and supervision. However, number of children who use internet in their own room is equally large, which allows for more personal and less supervised internet experience.

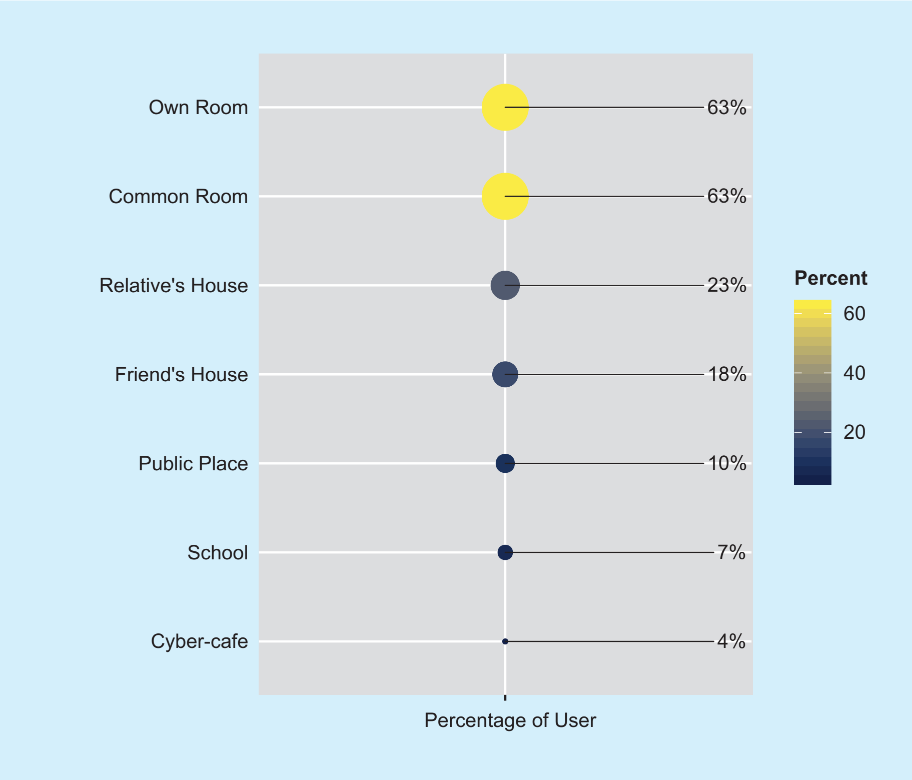


Figure 7: Place of internet use

This trend also indicates the prevalence of 'bedroom culture' as observed in other countries as well. Relatives' house (22%) and friends' home (17%) are respectively third and fourth most used locations.

When compared with European children (63%), only a small proportion of the children (7%) in Bangladesh are using internet at school. Interestingly, although cyber cafes were once a very common place for gaming and using internet, only a small proportion of the children today are going to the these places for accessing internet. Hence, the risks associated with using internet in cybercafé as observed in some other developing country is less intense for Bangladeshi children.

Device of Internet Access

Children were asked what kind of devices they used to access internet and who owned those devices. The respondents could provide multiple answers if they used multiple devices. Parents' smartphone is found to be most used device (49%) for accessing internet, followed by own smartphone (34%) and feature phone of parents (34%).

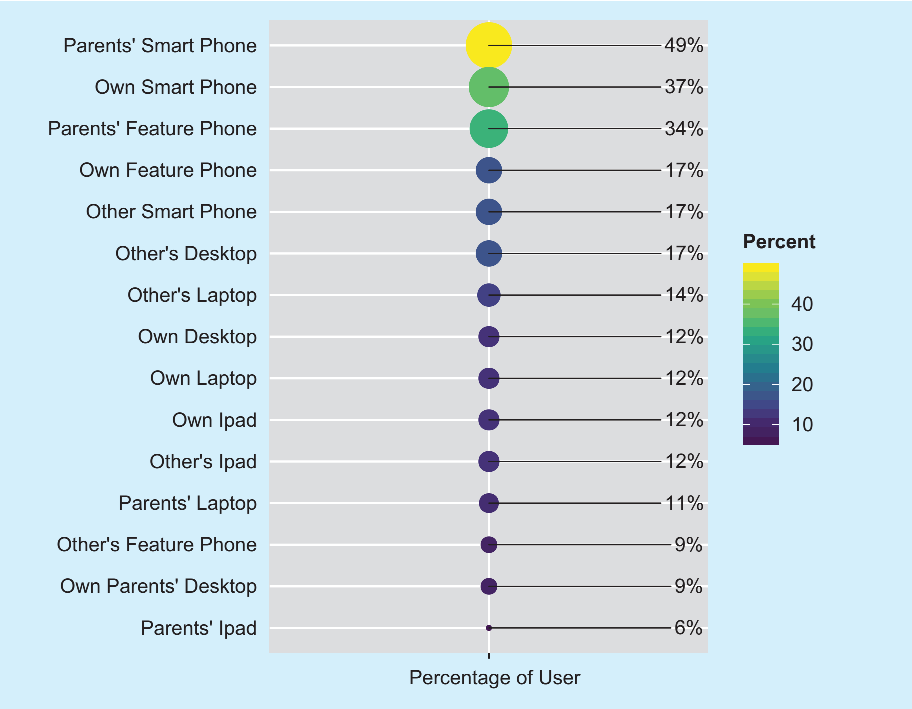


Figure 8: Device of use

Internet Usage Frequency

Forty percent (42%) of the participants said they use the internet every day, and 29% responded that they use between 2-5 days a week. A large number of respondents (22%) said that they access internet rarely which indicates that these children are missing out on the opportunities of exploring, learning and using internet.

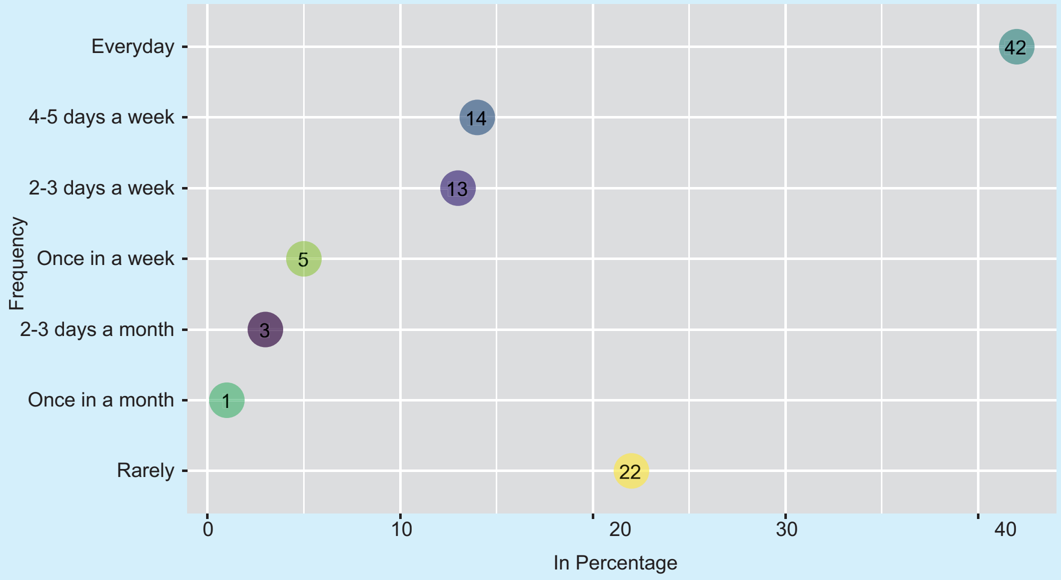


Figure 9: Usage Frequency

In order to determine differences in access frequencies among different groups of children, the responses were grouped into three broad categories;

Heavy Frequency User: Respondents who access internet ‘Everyday’

Medium Frequency Users: Participants who access ‘4-5 times a week’ or ‘2-3 times a week’

Light Frequency Users: Those who access internet once a week or less.

The figure below shows that boys (63%) are ahead of girls (48%) in terms of heavy frequency access. Besides, a higher proportion of girls can be classified as light frequency users. Hence, it can be interpreted that boys are more frequent users of internet than girls. Children of English medium background have an edge over those of Bangla medium and Madrasahs as 94% of them are heavy frequency users.

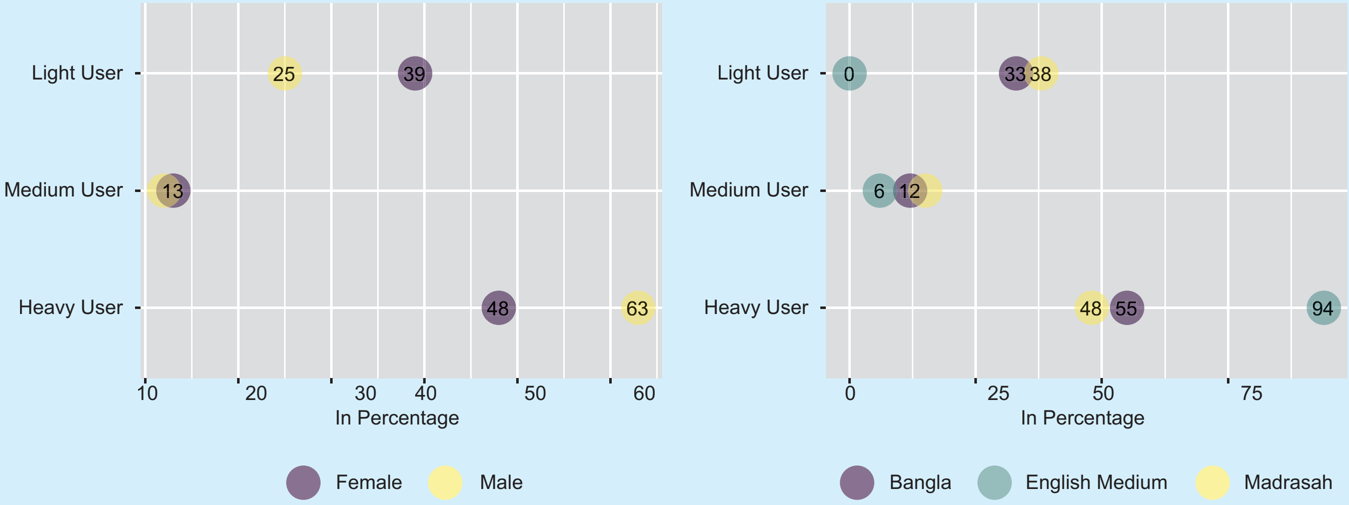


Figure 10: Usage Frequency of the respondents by sex and medium of school

2.3.2 **Practices**

This section will highlight different online activities performed by different groups of children in Bangladesh. Figure below shows what percent of all the children performs these activities every day. After presenting the broad insights, differences in online activities among different groups of children will be highlighted.

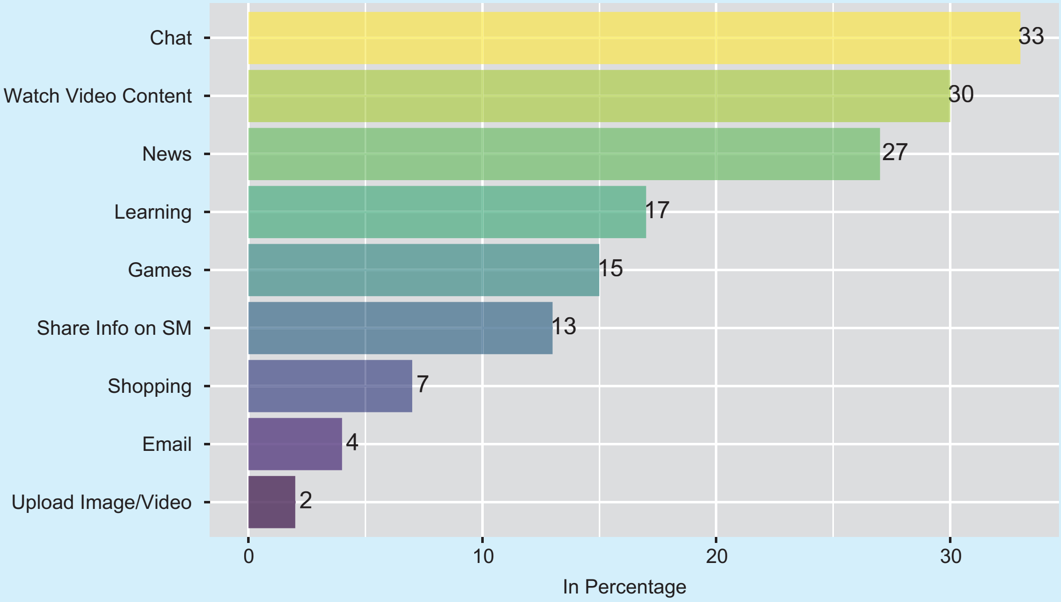


Figure 11: Daily online activities by the respondents

The figure 11 shows the daily engagement of different activities online, and chatting is the most frequent one. Thirty-three (33%) percent of the children stated that they chat online every day. Other frequent activities that children claimed to perform online every day were watching videos (30%) and reading news (27%). Few children aged 10 to 17 stated that they communicate over email (4%), and upload self-created video (2%). This is understandable since email communication is supposed to be less frequent, and uploading self-created video may be time consuming.

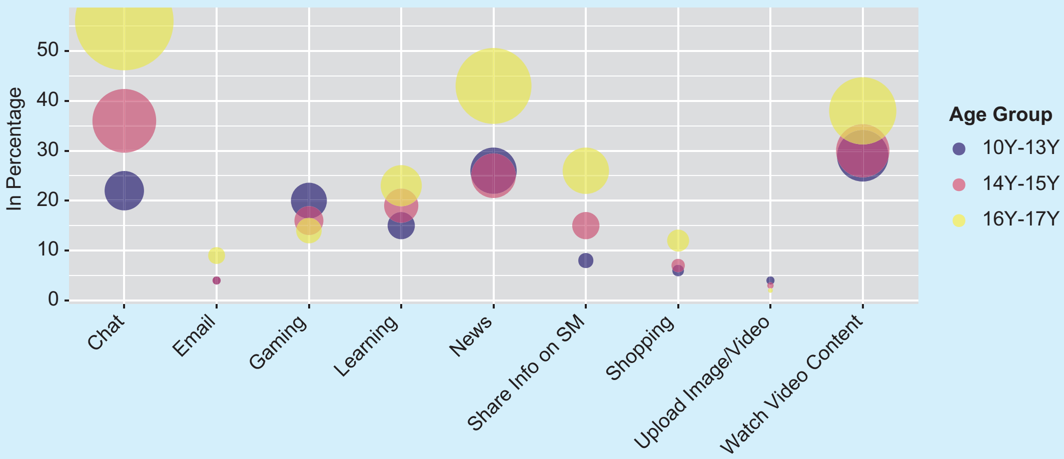


Figure 12: Daily activities by age groups

The figure 12 portrays age group wise segregation of different online activities. In majority of the online activities (7 out of 9), daily engagement is highest among the children aged 16 to 17. Chatting is more frequently performed by older children; 56% of the children aged 16-17, 36% of the children aged 14-15, and 22% of the children aged 10-13 chat every day. Same pattern can be observed for other activities including learning, social media activity, and looking for information for buying or selling online. The patterns is reversed for gaming.

Noticeable gender differences have been observed in all forms of online activities. Boys perform all forms of online activities more than the girls. Largest gender gaps can be observed in gaming, chatting and social media activities in favour of the boys. The figure below illuminates that girls are lagging behind boys in taking up the opportunities in the internet.

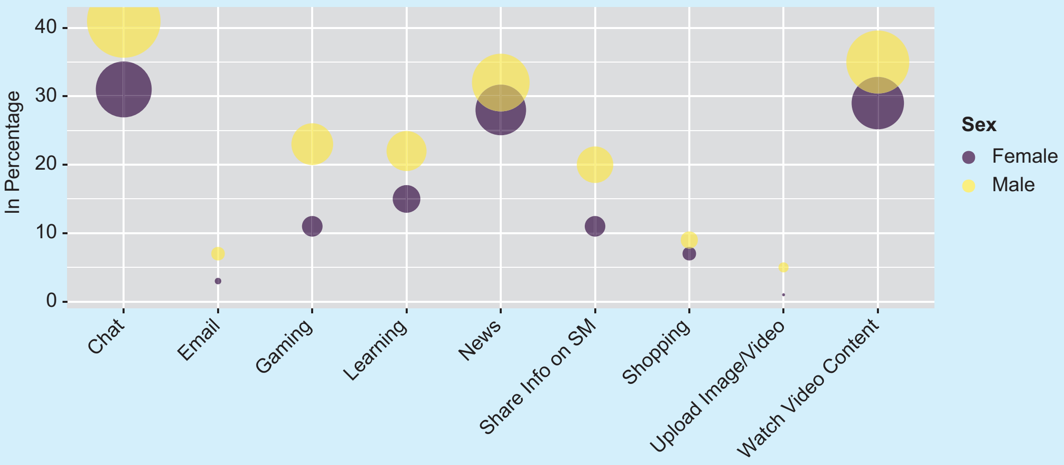


Figure 13: Daily internet activities by sex

In the area wise segregation, urban children's daily engagement is higher for majority of the online activities, but peri-urban children do not have clear edge over rural children.

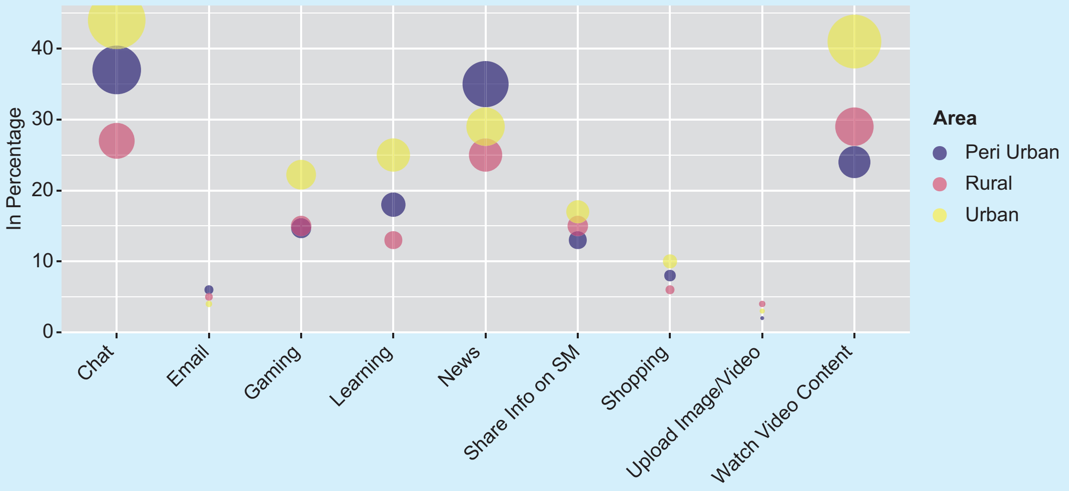


Figure 14: Daily internet activities by area

Social Media Use:

The current study explored social media usage by children in Bangladesh, hence, the respondents were asked whether they have account in a range of sites/apps. About 94% of the respondents have account in at least one of the sites or apps, with Facebook being the most popular among them (81%). Among the top five sites/apps, 2 are social networking and 3 are messaging apps. Few respondents said they have account in dating apps Tinder and Tantan. About 15% of the respondents said to have account in Tik Tok, a media sharing app. The app has been controversial in some countries, for instance, Indonesia temporarily banned it for allegedly containing pornography, inappropriate content and blasphemy.

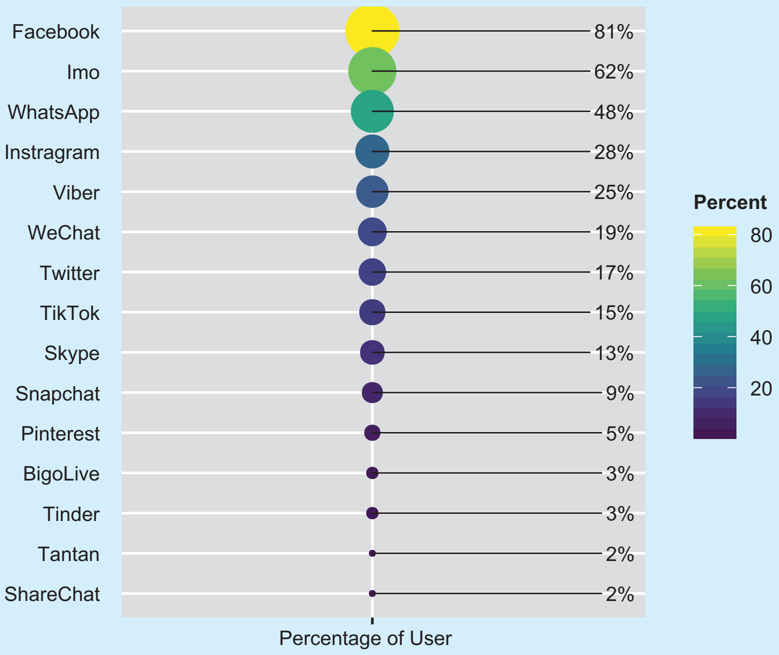


Figure 15: Respondents having Social media account

2.4 Online Safety Skills

Children require digital skills to fully experience the vast array of opportunities in the digital world while being safe from risks and harms. The baseline study investigated four safety skills; ability to change privacy setting of social media account, blocking message of an unwanted person, using 'report' option in social media account, and blocking pop-ups ads. Safety related skills do not automatically indicate how safe the children are, since application of these skills and awareness about online risks are equally important (this will be explored further in later sections of the report). Besides, children's self-reported perception of their own skills could also be different from actual skills that they have.

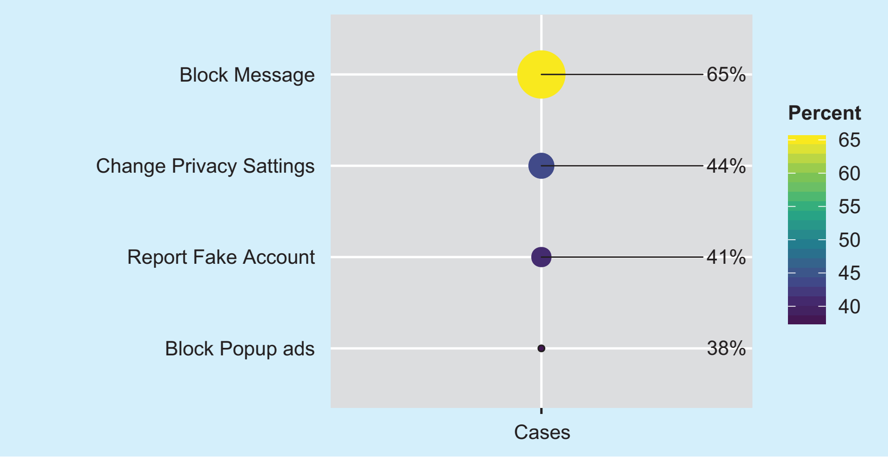


Figure 16: Online safety related skills

The figure 16 depicts that among all four skills, the ability to block message from unwanted people was highest (65%) among the children aged between 10 and 17. Only 44% stated that they can change the privacy setting and 42% stated that they know how to report something in the social media that they use. Skill deficiency was highest for blocking pop-up ads. Only 38% admitted that they know how to block pop-up ads.

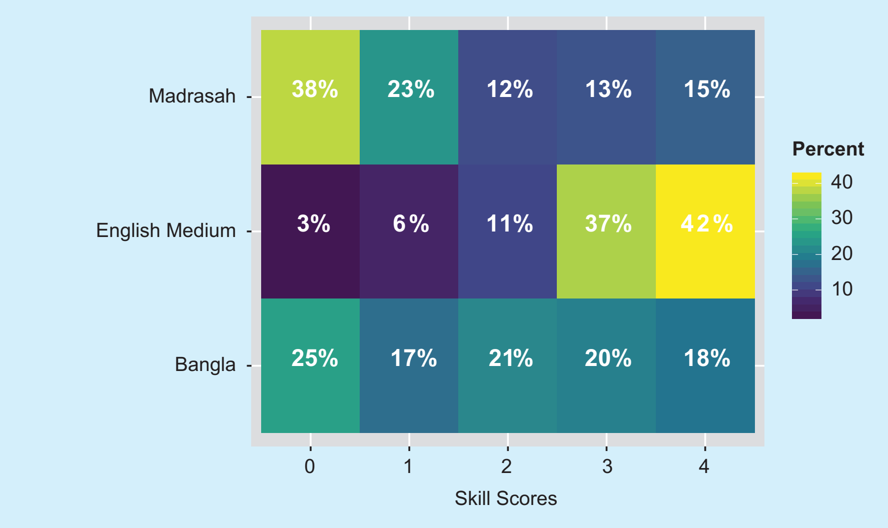


Figure 17: Online safety related skills by medium of education. The Skill score indicates the number of skills possessed by the children.

The online skills were transformed into skill scores for comparative analysis among different groups of children. The score indicates the number of skills possessed by the respondents. For instance, a skill score – '4' indicates that a respondent has all four skills, whereas a skill score '0' indicates no skill at all.

Regarding the Skill score, children from the English medium background are ahead of those in Bangla medium institutions and Madrasahs (see the figure 17). Almost four out of five students (79%) of the English medium students know at least 3 skills, compared with 38% of the Bangla medium students and 29% of the Madrasah students. Safety related skills are lowest among the children studying at Madrasahs as majority of them have only one skill or no skill at all.

Area wise comparative analysis portrays that skill deficiency is highest among the rural children of Bangladesh. Among the rural children, 38% do not have any of the four safety skills, compared with 15% of the urban and 23% of the peri-urban children. Seventy-one per cent (71%) of the rural children reported to know two skills or less, whereas 47% of the urban and 66% of peri-urban children said so. Safety related skill gap of the peri-urban children is lower than the urban children, however, they have more skills than those at the rural areas.

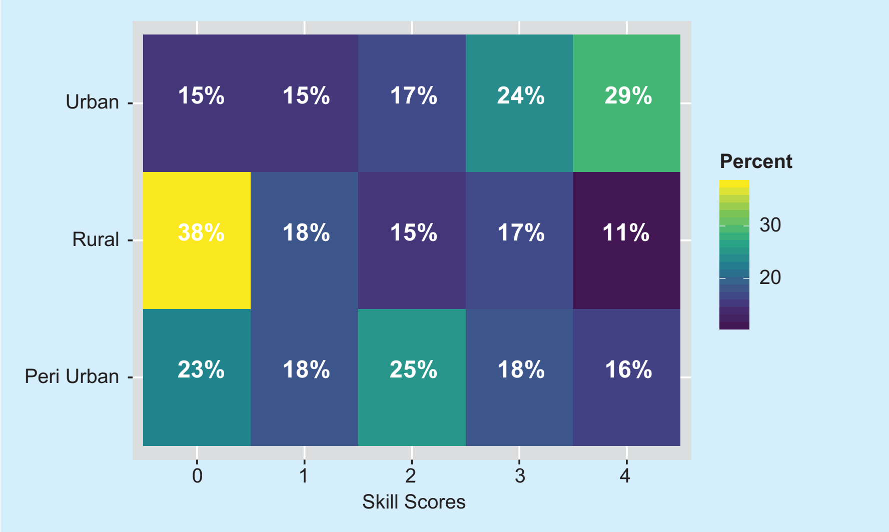


Figure 18: Online safety related skills by area. The Skill score indicates the number of skills possessed by the children.

2.5 Risk and Harms

2.5.1 Risky Online Behaviour

Children often through their own activities can be exposed to different kinds of online risks, and those activities have been explored in the section. Risky activities investigated in the research relate to sharing of private information and communicating (online or offline) with strangers. Due to the nature of these activities, children in these behaviors can be assumed to be at more risk than those who do not. For example, sharing private information (home address, mobile number, etc.) with an online contact can be regarded as a risky behavior, although such behavior does not always bring harm upon children.

Sharing of private information or content with online acquaintances:

A total of 10.8% children said that they had sent their personal information (address, phone number etc.) to an online acquaintance within one year preceding the study. Some 12.3% admitted that they had sent family information and 11.7% reported that they had shared their own images or videos with an online acquaintance within one year preceding the study.

The figure 20 indicates boys are involved in more risky activities with regards to sharing personal information and own image or video. However, boys' tendency to share family information is slightly lower than that of girls.

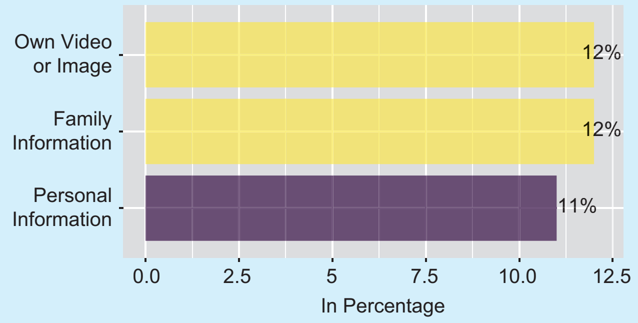


Figure 19: Proportion of the respondents sharing private information and content with online acquaintance

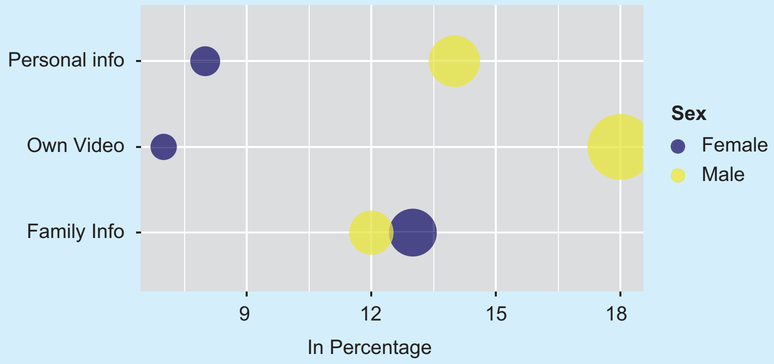


Figure 20: Sharing of private information with online acquaintance, by sex

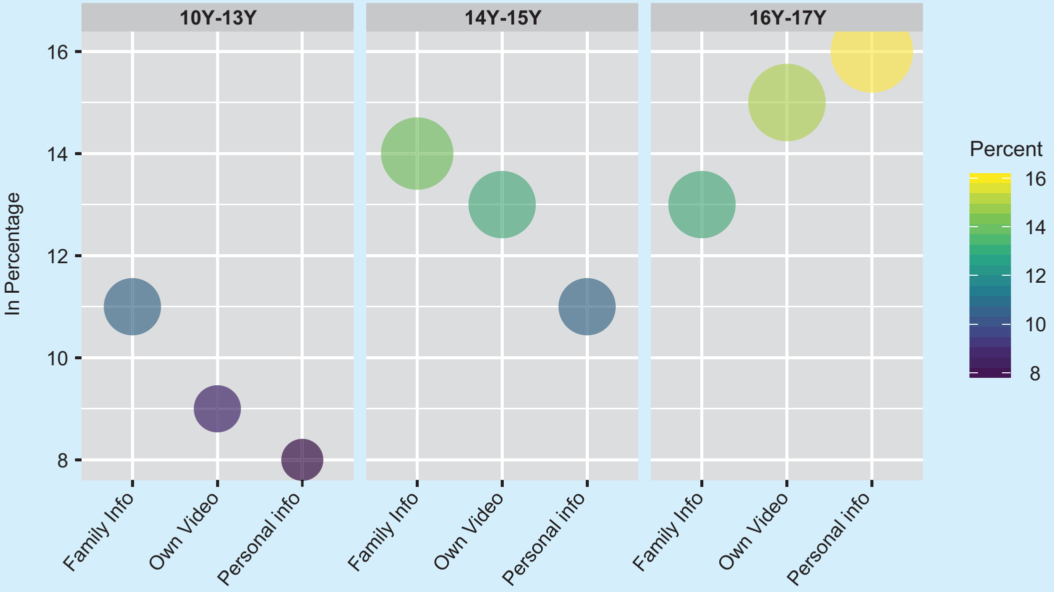


Figure 21: Sharing of private information and content by age group

When children's involvement in different risky behaviour was analyzed by their age groups, no uniform pattern was visible. Children belonging to the age group '10-13' generally engage at lesser extent than other children in three forms of risky online behaviours; sharing personal information (8%), sharing family information (11%), and sharing own image or video (9%). The figure 21 shows that a higher proportion of children aged 16 and 17 share their personal information (16%) and own images and videos (15%) with online acquaintances.

Password Sharing

It is important to understand children's knowledge and awareness about protecting passwords of their email, social media or any other account that use in the internet. To understand the level of awareness among children about the secrecy of passwords, they were asked whether they had ever shared their password with anyone. The purpose of the question was to comprehend their level of awareness through their self-reported action. Overall, 34% of the respondents shared their password with someone else, and 24% said they shared with their parents or siblings. Ten percent (10%) of the respondents shared their password with people other than parents or siblings, and therefore, it can be interpreted that 10% of children lack the awareness about the importance of password protection.

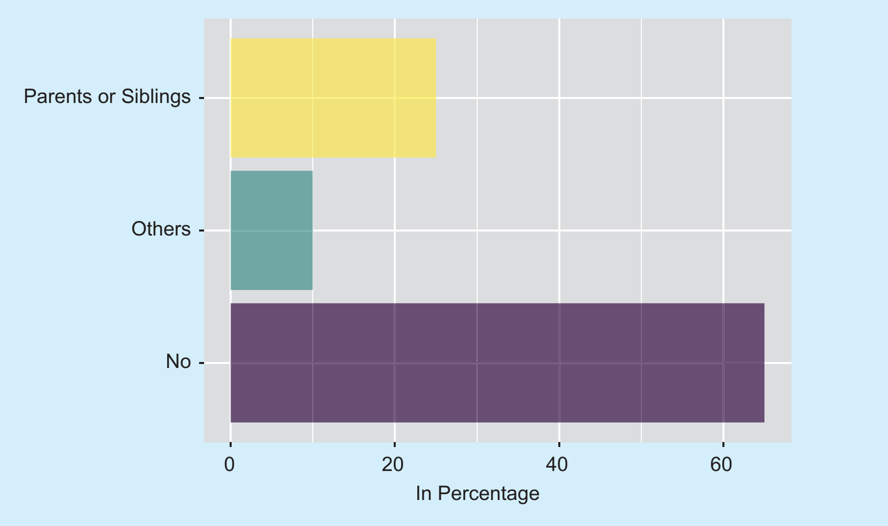


Figure 22: Password sharing

Contact with Online Acquaintances

Majority of the respondents (57%) stated that they befriend unknown people in the internet. It was interesting to explore what forms of communication do children establish after befriending an unknown person online. Therefore, the survey questionnaire asked whether they had talked with an online acquaintance over the phone, over video call, and whether they had met with an online acquaintance in person.

Twenty-seven percent (27%) of all respondents said that they talked with someone over the phone after getting acquainted with him/her in the internet, and 17% said they talked over video call with an online acquaintance. Probably the riskiest among all the three mentioned behaviour is meeting an online contact in person, and a staggering 14% of the children said they had met with an online acquaintance.

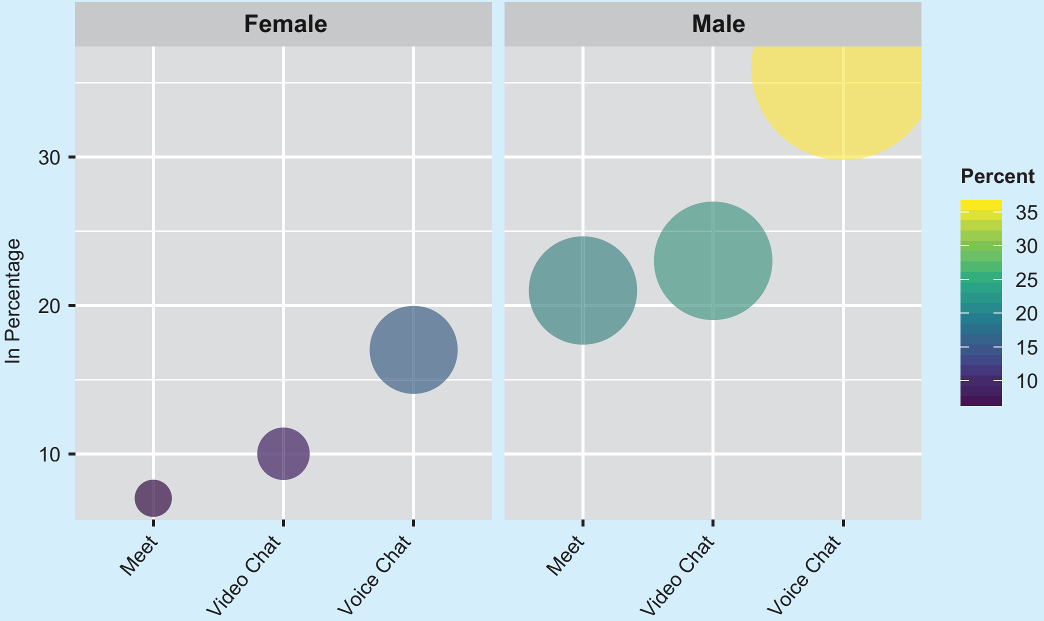


Figure 23: Contact with online acquaintances by sex

As regards gender, boys' involvement in all forms of contact with online acquaintances is higher than the girls. Thirty-six percent (36%) of boys talked with an online acquaintance, while 17% of girls did so. As to video call, 23% of the boys said that they communicated with an online acquaintance when only 9% of the girls said they did so. Nearly 14% more boys than girls met with an online acquaintance face to face.

As to age, older children showed higher tendency in forming different forms of contact with an online acquaintance. Forty-two percent (42%) of the children aged 16 to 17 talked with an online acquaintance over the phone, compared with 28% of children aged 14-15 and 17% of the children aged 10-13. Some 24% of the children aged 16-17 communicated with an online acquaintance over video call, a figure that exceeds that of children aged 14-15 by 9 percentage points, and that of children aged 10-13 by 14 percentage points. Children belonging to the age group 16-17, showed a higher tendency (18%) in meeting an online acquaintance face to face than those of the age group 14-15 (14%), and 10-13 (11%).

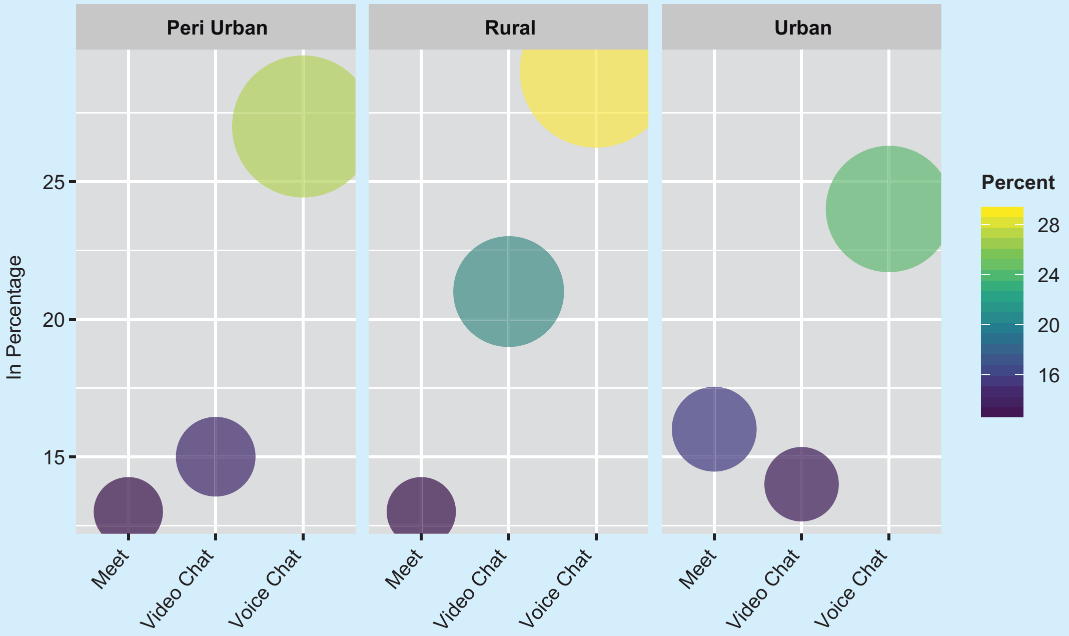


Figure 24: Contact with online acquaintances by age group

2.5.2 **Risk Related to Sexually Inappropriate Content**

Children can be exposed to content risks, being recipient of inappropriate sexual message, videos, and images. The senders of these sexual contents could be either adults or other children. The current study tried to investigate the sexual risks from two angles; child as recipient, child as an active participant.

Child as Recipient

Around 19% of the respondents said that they had received sexual text while using internet within one year preceding the study. Twelve per cent (12%) of the children received sexual images or videos online within one year preceding the study. Therefore, it can be said that large number of children are getting exposed to sexual contents. These two forms sexual risks have been separately analyzed to determine whether the degree of exposure to sexual contents is different among different groups of children.

Sexually Inappropriate Message

Boys (24%) reported to receive sexually inappropriate message more than girls (14%) did. Notable difference in exposure to sexually inappropriate messages was found among children of different schooling system. Thirty percent (30%) of children from English medium schools claimed to receive sexual message, while 20% of Bangla medium and 14% of Madrasah children did so.

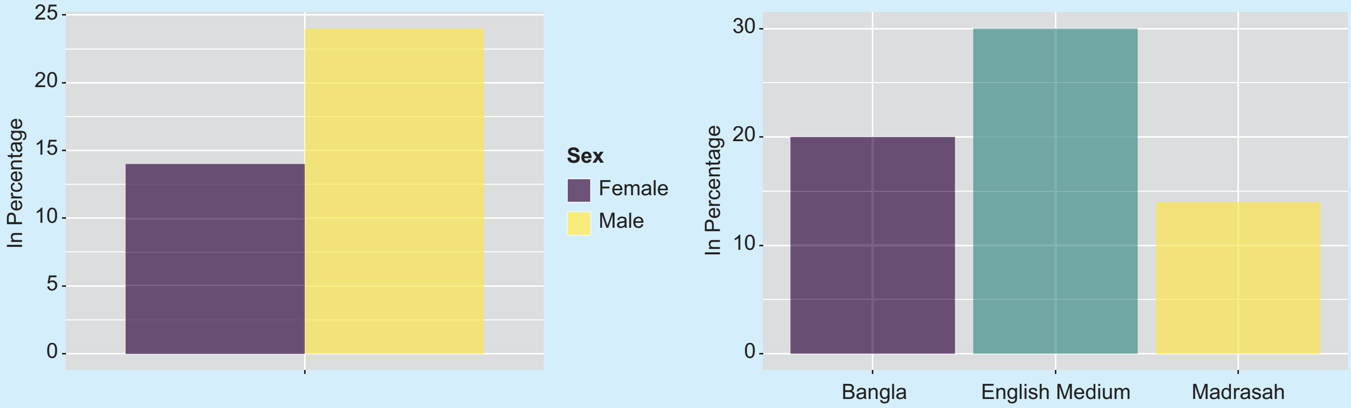


Figure 25: Receiving sexually inappropriate message by gender and medium of education.

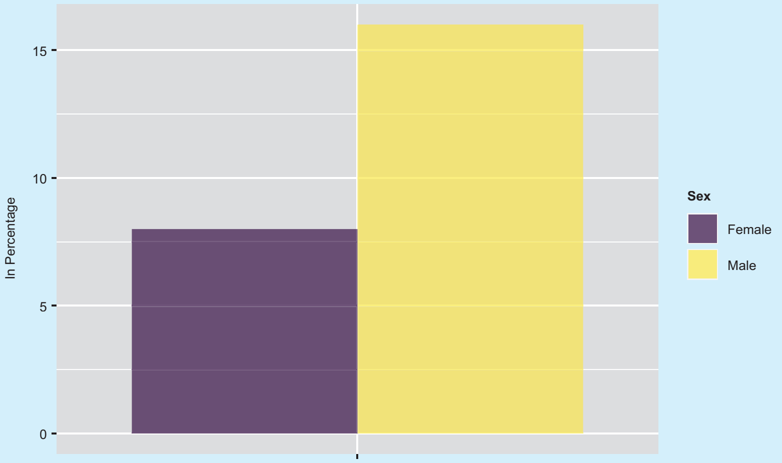


Figure 26: Receiving sexually inappropriate image or video by sex

Sexual Image or Video: As to gender, percentage of boys (16%) who received sexual image or video was twice that of the girls (8%). This finding is consistent with that of sexual text. Boys receive sexual text and other forms of sexual contents more than girls do. With reference to schooling system, no difference was found among different groups of children.

Child as an Active Participant

In order to explore active participation by children in spreading/sharing sexually inappropriate content, the respondents were asked whether they had sent sexual image, text or video to someone, and whether they had posted any such content on any website or on any social networking site within one year before the study. The number of children who said ‘Yes’ to these two questions was very low. Only around 2% of the children said they had sent sexual content to someone, and 1% of them shared sexual content online.

Being asked or Insisted to Send Own Nude/Semi-nude Image or Video

Sending sexual image or video of their own self with someone online is probably one of the biggest sexual risk for children at least theoretically. Children who share these contents could easily fall victim of sexual abuse or exploitation if things go wrong. However, asking the children directly whether they had sent their own nude/semi-nude image or video would be very sensitive. Rather the survey question was whether they had been asked or had been insisted by anyone to send their own nude or half-nude image or video in one year preceding the study. Five per cent (5%) of all the children aged between 10 and 17 stated that someone had asked or insisted them to send their own naked or half naked image or video. Whether such persuasion has been done by a romantic partner or by an adult who intent on abusing or exploiting the child, this figure is very alarming.

Exposure to Sexually Inappropriate Content by Divisions

Children from Khulna and Rajshahi and Dhaka have been more exposed to three forms of sexual risks; receiving inappropriate content (image or video), receiving inappropriate text, and being asked or insisted to send own nude/semi-nude image or video. Overall responses to other two items (sending or sharing inappropriate content) were very low, hence, division wise difference do not provide much insight.

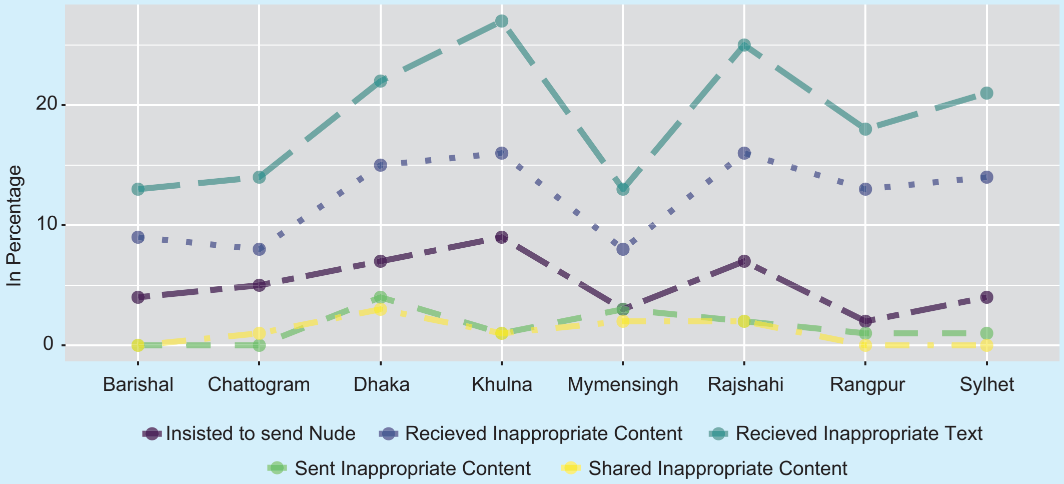
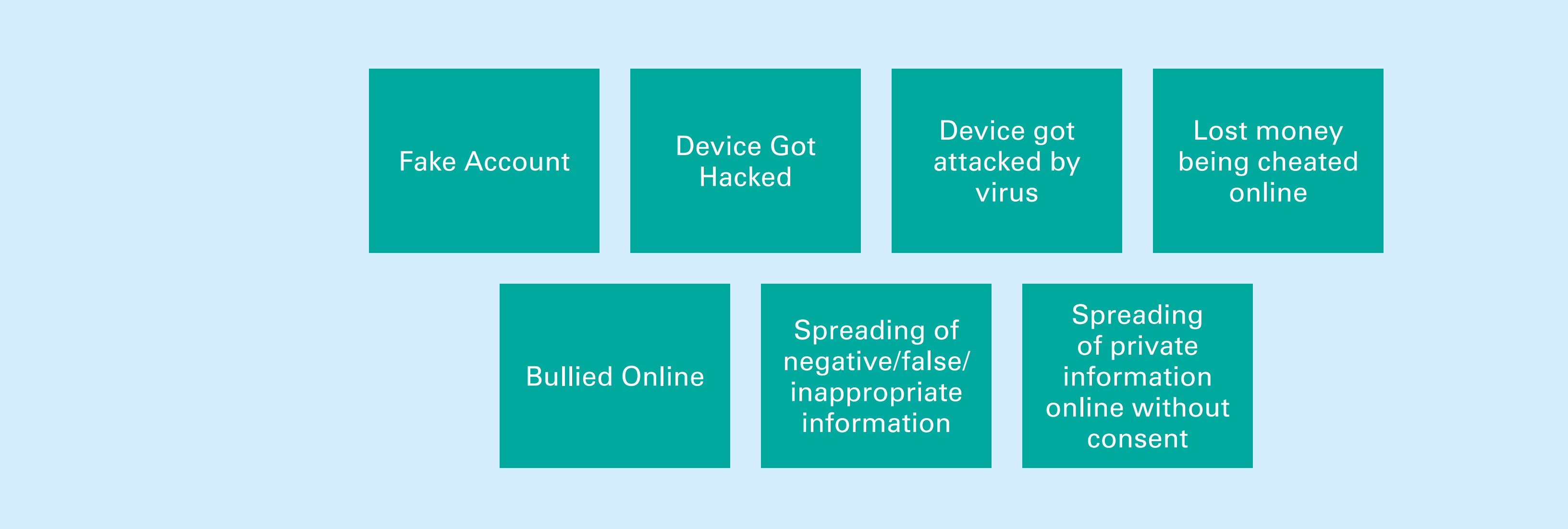


Figure 27: Exposure to sexually inappropriate content by division

2.5.3 **Online Harms**

It is important to distinguish between risks and harms in the internet as every event of risk may not materialize into a harmful or negative experience for the children. Literature review of the study reveals that occurrence of actual harm may depend on various other factor including the type of the risk and the country context. This section of the report illuminates actual negative experiences or harms for children in the internet. A total of 7 questions were asked related to types of negative experiences, some of which might create greater negative impact on children than others. None of the question specified time period, hence, these negative experiences could have happened any time.



Fake Account

Device Got Hacked

Device got attacked by virus

Lost money being cheated online

Bullied Online

Spreading of negative/false/ inappropriate information

Spreading of private information online without consent

Figure 28: Types of online harms explored in the study

The figure below presents an overview of different types of online harms experienced by children in Bangladesh. Virus attack is the most prevalent harm, with some 37% of the respondents saying their device got infected with virus sometime. The second most reported harm is cyber bullying as almost 3 out of 10 respondents (32%) claimed that they had been bullied sometime over the internet. Some 16% of the children reported that their account (social media, email etc.) got hacked sometime. This high figure is alarming since these children may be at the risk of losing their private information which could lead to even bigger harms. However, the figure may be inflated if incidents such as forgetting password are misinterpreted by children as being hacked. Thirteen per cent (13%) of the children experienced opening of fake account in the social media, while similar percentage said that nasty and fake information about them are spread online.

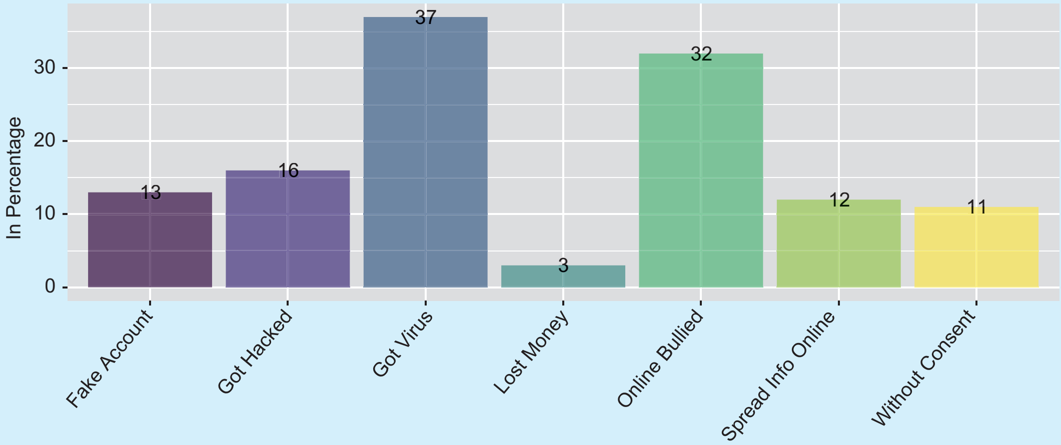


Figure 29: Frequency of online harms by age

With regards to gender, boys experienced all forms of harms more than girls except for opening of fake account. Biggest gender gaps can be seen in the experience of virus attack and online bullying. Some 46% of the boys said that their device got infected by virus, a figure which exceeds that of the girls by 17 percentage points.

Regarding cyber bullying, forty per cent (40%) of the boys experienced at least one form of cyber bullying, whereas for girls the figure was 24%. Attribute risk was 15.39% for boys, showing that boys have 15.39% more probability of getting bullied than girls. As to the experience of account hacking, the relative risk of boys being hacked is 1.5 times higher.

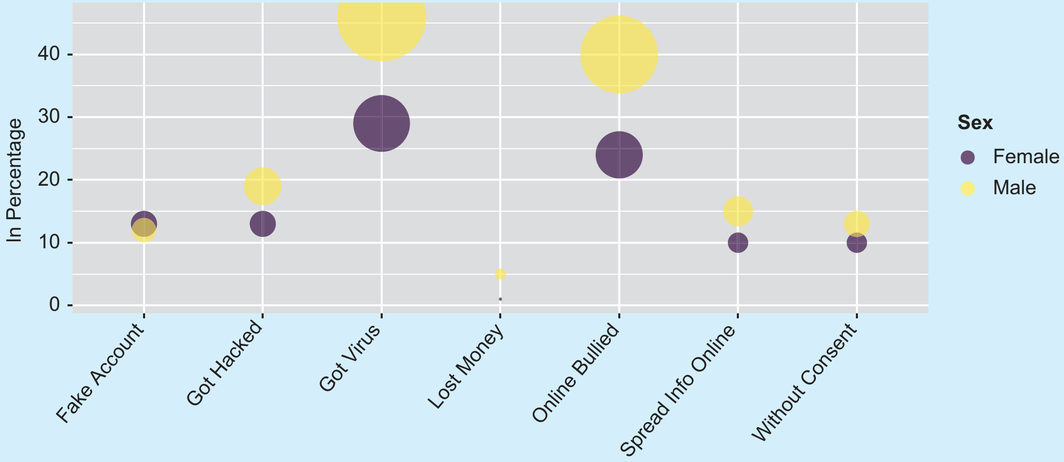


Figure 30: Frequency of online harms by sex

As to age, the oldest group of children (16-17) experienced all forms of online harms more than younger groups of children did. Comparison of the two younger groups shows that, children aged 14 to 15 are more exposed than are youngest children for majority of the online harms.

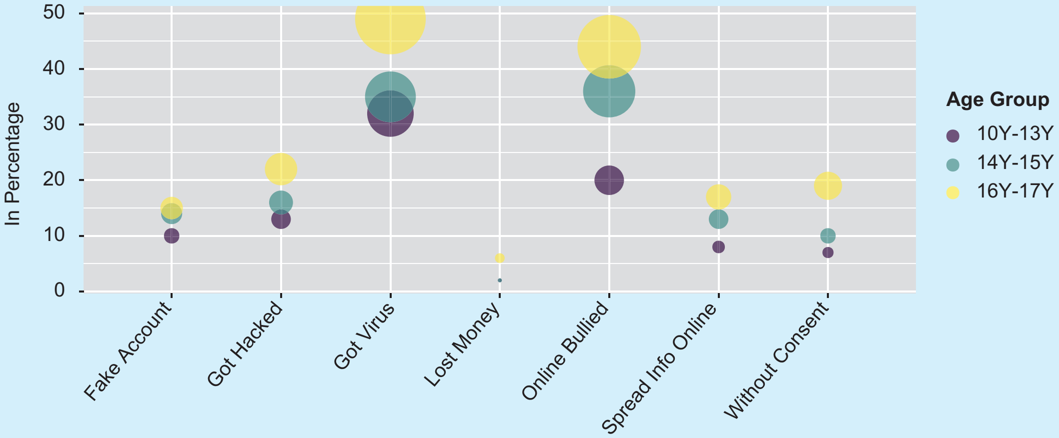


Figure 31: Frequency of online harms by age group

Segregation based on area indicates that urban children experienced four out of seven forms of harms more than other children; opening fake account, virus attack, spreading of nasty or fake information, and sharing private information/image/video without consent. Forty-four per cent (44%) of the urban children said their device got infected by a virus, which is 9 percentage points higher than that of peri-urban children, and 11 percentage points higher than that of rural children. With regards to fake account, 17% of urban, 12% of peri-urban and 9% of rural children experienced such harm. The percentage of urban children who stated that their private information/image/video had been shared without their consent was 4 points higher than that of peri-urban and rural children.

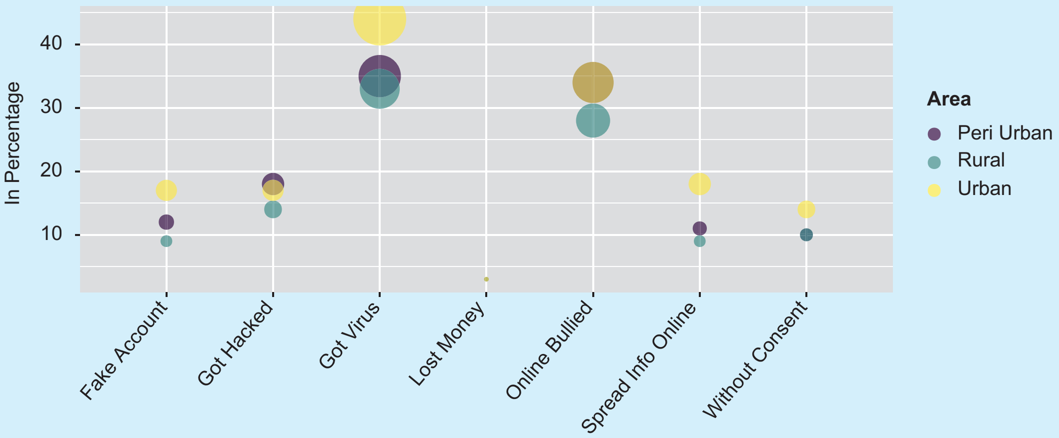


Figure 32: Frequency of online harms by area

2.5.4 **Religious Provocation**

Assessing the risk of cyber extremism through survey alone is difficult since children might not be able to distinguish between harmless religious preaching and extremist ideologies. Therefore, the study only explored children's own perception about facing religious provocation. Children were asked if they had ever received religiously provocative message, image or video in the internet. About 10% of the respondents claimed that they had received such religiously provocative content online.

As to age, children of the oldest group are more exposed to religious provocation than younger children. Fifteen percent (15%) of the children aged 16-17 received religiously provocative text, image or video when only 8% of the children aged 14-15 and 7% of the children aged 10-13 did so. Among the participants, boys tend to receive such religiously provocative content more than the girls do. Percentage of boys who received such content was almost three times that of girls, hence, boys are at more risk than girls.

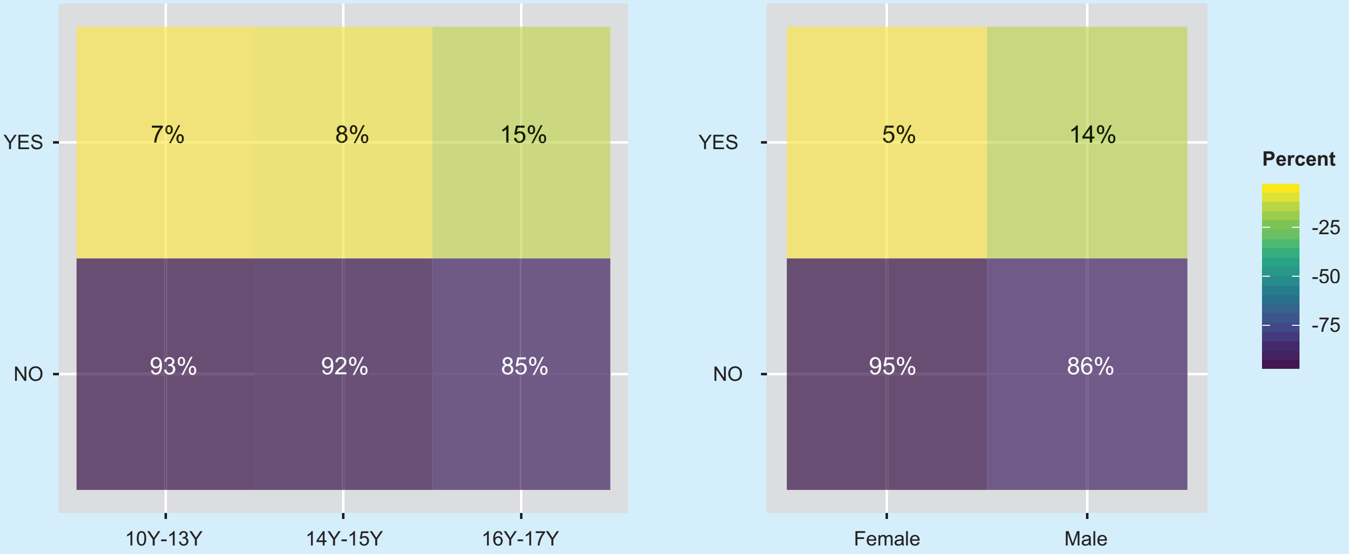


Figure 33: Receiving religiously provocative content by age and sex

2.6 Coping and Social Mediation

The study explored who children turn to for help if they experience any negative experience online, and what role parents/guardian play in mediating their internet activities. Both the help seeking behaviour of children and mediation by parents/guardians are important to understand the level of vulneribily, since some children may have less support system available to them than others have.

2.6.1 **Help Seeking Behaviour**

Gender wise segregation shows that boys are either more confident about their ability, or are more reluctant in seeking support. More boys (28%) said they would solve their own problem than girls (15%). Only small percentage of the both boys and girls said they would do nothing, but, the responses was higher in favor of the boys. Parents/guardians are generally the most favoured support group, as some 67% of the girls would ask help from their parents/guardians, and around 50% of the boys said they would do so.

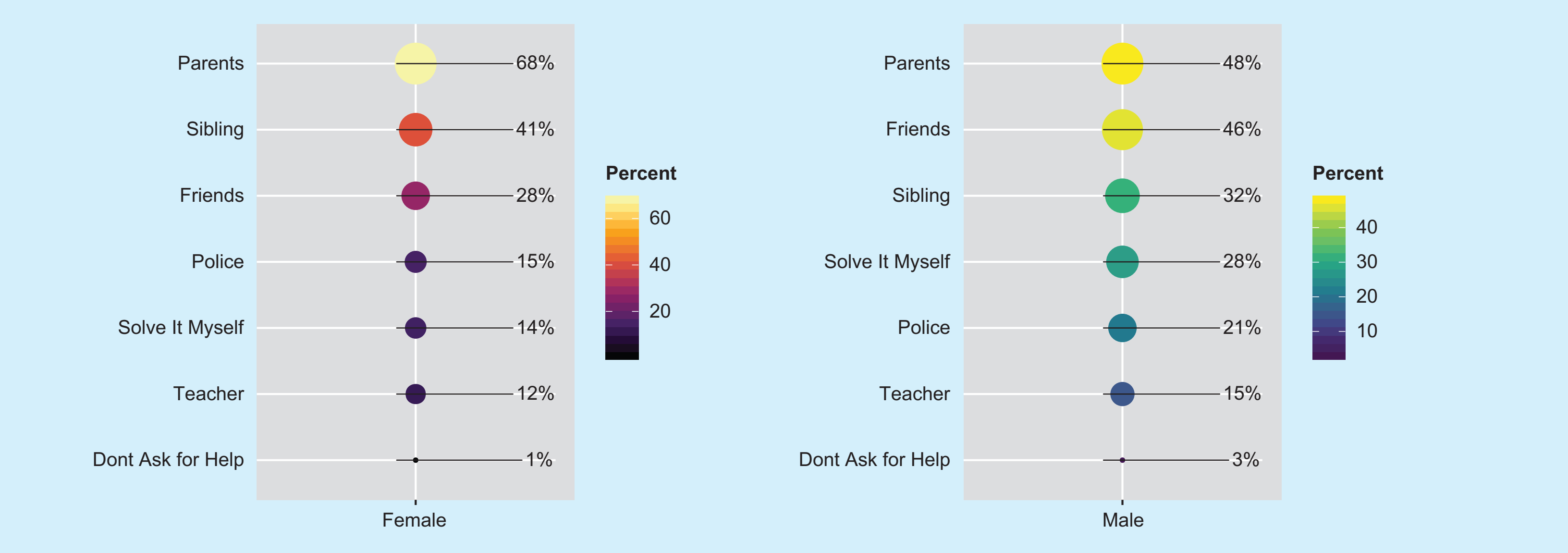


Figure 34: Seeking help after online harm by gender

Other than gender, little difference was observed in support seeking behaviour among different groups of children.

2.6.2 **Mediation by Parents/Guardians**

Role of parents/guardians are important not only because they are the first level of support for the children when they face any risk/harms, but also because they are have the primary responsibilty in keeping children off online harms. The survey questionnaire asked three questions to the respondents related to different types of mediation ; how frequently parents/guardians suggest ways to use internet safely, set rules for internet usage, and monitor internet activities.

Active Mediation

Children were asked whether their guardians[12] suggest them ways to use internet safely. Gender wise segregation (figure 35) shows that a staggering 32% of the boys are 'never' taught by their guardians about safe use of internet, and for girls the figure is 19%. Notable difference was observed with regards to schooling system. Four out of ten children from Madrasahs said they are 'never' taught about the safe use of internet by their guardians, while only 23% of the Bangla medium students and 22% of the English medium students said so. Morever, the proportion of Madrasah children who are 'always' guided by their guardians is only 21%.

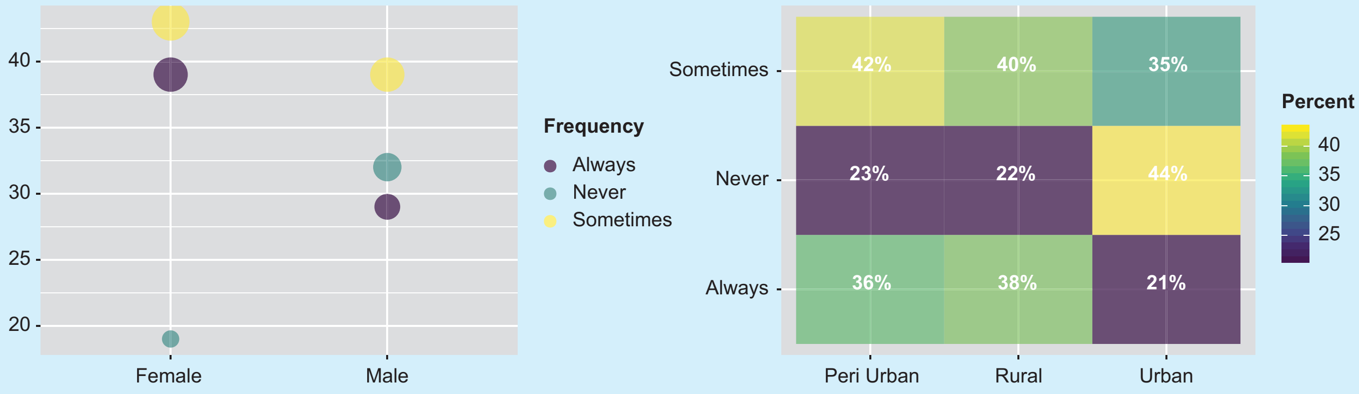


Figure 35: Guardians suggesting safe internet use by sex and schooling system

As to age, guardians' involvement in educating safe use of internet goes down as children become older. The figure 36 shows that as we move from younger to older age groups, the percentage of children who are 'always' guided by guardians drops sharply.

[12] Actual question in the questionnaire asked the role of parents/guardian. For better readability, this section uses the term 'guardian' only.

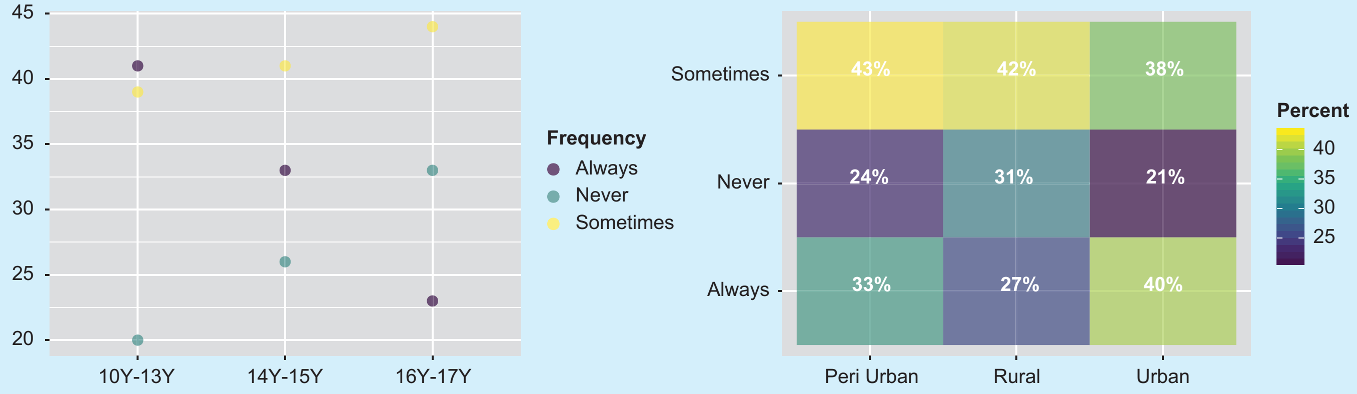


Figure 36: Guardians suggesting safe internet use by age groups and area

Besides, increasingly larger proportion of children are 'never' taught about safe use of internet as we move towards older groups of children.

As to area, rural children experience less guidance from guardians. Thirty per cent (31%) of rural children are never guided by than that of peri-urban(24%) and urban children(21%).

Other Forms of Mediation

Rule Setting

The survey questionnaire asked the children whether their guardians set rules of any kind for using internet. According to the figure below, girls experience such restriction more than the boys do. Among all the girls, 34% are 'always' bound by some rules by their guardians for using internet, a figure that exceeds that of the boys by 9 percentage points. Besides, the percentage of girls (28%) who are 'never' restricted by any rule is much lower than that of the boys (39%).

With regards schooling system, children from Madrasahs face little restriction compared to students from other two medium. A staggering 48% of the children from Madrasahs stated their guardians 'never' set any rule for them regarding internet usage. As to area, rural children face little restriction when compared with the children of urban and peri-urban areas. Four out of ten rural children said their guardians never set rule for their internet usage, which is a stagering number.

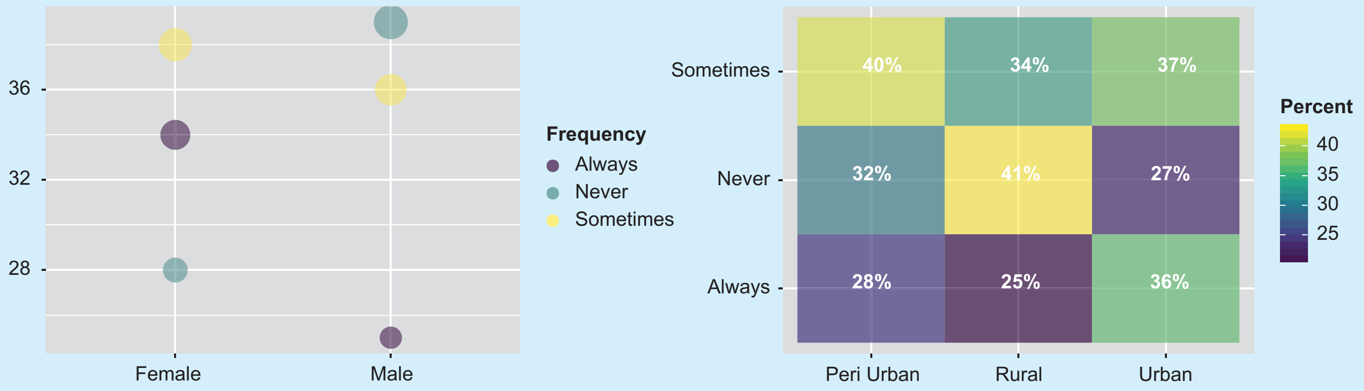


Figure 37: Setting rule for internet usage by sex and area

Monitoring

The current study also investigated whether guardians monitor internet activities of their children. According to the figure 38 , internet activities of girls are monitored more than that of boys. Twenty four per cent (24%) of the girls said that their internet activities are 'never' monitored by their guardians, while thirty-two per (32%) cent of the boys said so. Percentage of girls who face monitoring by guardian 'sometimes' or 'always' is also higher than that of the boys. With regards to schooling medium, children from the English medium schooling background face monitoring less than other children. About half the English medium students stated that they 'never' face any parental monitoring of their activities in the internet.

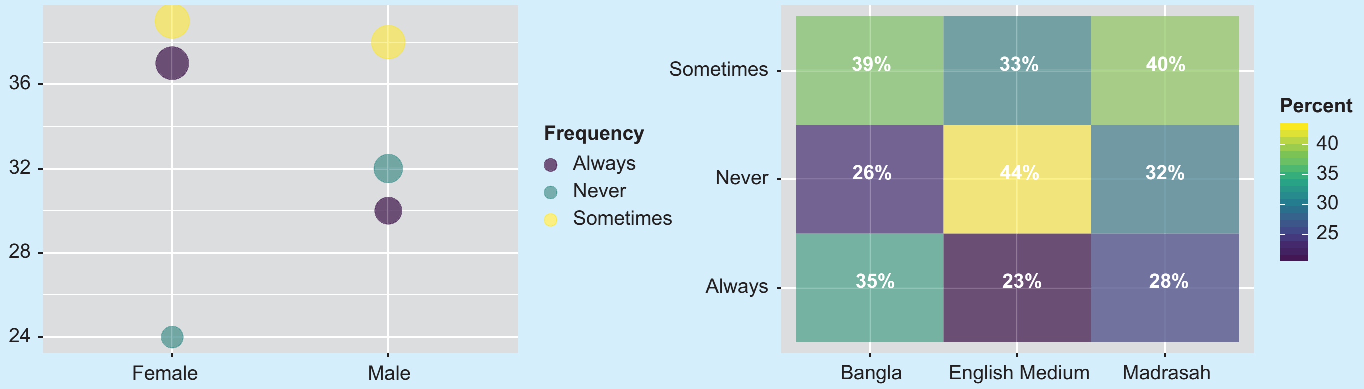


Figure 38: Parents' monitoring of internet usage by medium of education and sex

Part 1 **Bibliography**

BDNEWS. (2018, March 31). *bdnews24.com*. Retrieved from https://bdnews24.com/technology/2018/03/31/childrens-perspectives-on-the-safe-internet-campaign

bdnews24.com. (2018, March 31). Children's perspectives on a 'safe internet'. *bdnews24.com*. Retrieved October 8, 2018, from Bdnews24.com: https://bdnews24.com/technology/2018/03/31/childrens-perspectives-on-the-safe-internet-campaign

Bergman, G. (2016). *Ethical considerations for research with children.* London: Global Kids Online. Retrieved from http://www.globalkidsonline.net/ethics

Berman, G. (2016). *Ethical Consideration for Research with Children.* Global Kid Online.

Financial Express. (2014, November 10). One in 3 Indian youth cyberbullied due to risky online behaviour: McAfee report. *Financial Express*. Retrieved October 5, 2018, from https://www.financialexpress.com/industry/technology/one-in-3-indian-youth-cyberbullied-due-to-risky-online-behaviour-mcafee-report/7392/

Ghosh, M. (2018, July 11). *Internet Browsing Habits Among Indian Children Are Worrisome & Alarming!* Retrieved from Trak.in: http://trak.in/tags/business/2015/05/26/internet-browsing-habits-indian-children-worrisome-alarming/

GLOBAL KIDS ONLINE ARGENTINA. (2016). *Research study on the perceptions and habits of children and adolescents on the use of technologies, the internet and social media.* Retrieved from http://eprints.lse.ac.uk/71284/

Govidnappa Lakshmana, S. K. (2018). *Internet Use Among Adolescents: Risk-Taking Behavior, Parental.* Retrieved from http://www.indjsp.org/temp/IndianJSocPsychiatry334297-8634338_235903.pdf

Hasebrink, U., Gorzig, A., Haddon, L., Kalmus, V., & Livingstone, S. (2011). *) Patterns of risk and safety online: in-depth analyses from the EU Kids Online survey of 9- to 16-year-olds and their parents in 25 European countries.* LSE, London: EU Kids Online network.

Kabir, A. (2018, January 26). Cyber radicalisation thrives in absence of cyber hygiene. *Prothom Alo*. Retrieved October 9, 2018, from https://en.prothomalo.com/bangladesh/news/170105/Cyber-radicalisation-thrives-in-absence-of-cyber

Lakshmana, G., Kasi, S., & Rehmatulla, M. (2017).). Internet use among adolescents: Risk-taking behavior, parental supervision, and implications for safety. *Indian J Soc Psychiatry, 33*(4), 297-304.

Livingstone, S., Haddon, L., Gorzig, A., & Olafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full Findings.* LSE, London: EU Kids Online.

Lobe, B., Livingstone, S., Olafsson, K., & Vodeb, H. (2011). *Crossnational comparison of risks and safety on the internet: initial analysis from the EU kids Online survey of European children. EU Kids Online, Deliverable D6.* London: EU Kids Online Network.

McAfee. (2013). *DIGITAL DECEPTION: THE ONLINE BEHAVIOUR OF TEENS.* United Kingdom. Retrieved from https://www.anti-bullyingalliance.org.uk/sites/default/files/field/attachment/mcafee_digital-deception_the-online-behaviour-of-teens.pdf

Optem. (2007). *Safer internet for Children: Qualitative study in 29 European countries- Summary report.* Brussels: Eurobarometer. Retrieved from http:www.beat.cat/documents/safer.pdf

PALO, H. (2018). *ONLINE SAFETY TOOLKIT FOR ADOLESCENTS IN RURAL NEPAL .* Kathmandu. Retrieved from http://www.her-turn.org/new/wp-content/uploads/2018/02/Online_Safety_Toolkit_English.pdf

Phyfer, J., Burton, P., & Leoschut, L. (2016). *South African Kids Online: Barriers, opportunities and risks. A glimpse into South African children's internet use and online activities. Technical Report.* Cape Town: Centre for Justice and Crime Preventation.

Professor Sonia Livingstone, P. J. (2017). *Children's online activities, risks and safety.* UKCCIS Evidence Group. Retrieved from http://www.lse.ac.uk/business-and-consultancy/consulting/assets/documents/childrens-online-activities-risks-and-safety.pdf

Rashid, M. M. (2017). *ONLINE RADICALIZATION: BANGLADESH PERSPECTIVE (master's Thesis).* Kansas: U.S. Army Command and General Staff College.

Richards, M., & Morrow, V. (1996). Ethics of Social Reearch with Children: An Overview. 90-105.

Singh, N., & Bishnoi, K. (2016). *Child Online Protection.* New Delhi: UNICEF.

Stoilova, M. (2018, February 8). *Making the internet safer for children: the global evidence.* Retrieved from Global Kids Online: http://globalkidsonline.net/safer-internet-day-2018/

Study: Internet users in Bangladesh have increased 800x since 2000. (2018, October 23). *Dhaka Tribune*. Retrieved from https://www.dhakatribune.com/bangladesh/2018/10/23/internet-usage-increasing-across-asia

Study: Internet users in Bangladesh have increased 800x since 2000. (2018, Octobber 23). Retrieved from Dhaka Tribune: https://www.dhakatribune.com/bangladesh/2018/10/23/internet-usage-increasing-across-asia

Tan, M., Estacio, L., & Ylade, M. (2016). *Global Kids Online in the Philippines. Country Report.* Manila: University of the Philippines Manila. Retrieved from www.globalkidsonline/philippines

The Economic Times. (2017, April 26). More Indian children visiting 'inappropriate' websites: Survey . Retrieved from https://economictimes.indiatimes.com/news/politics-and-nation/more-indian-children-visiting-inappropriate-websites-survey/articleshow/58385339.cms

The New Indian Express. (2018, october 7). Online child sexual abuse on the rise. Child sexual abuse is not a myth but a horrifying reality. *The New Indian Express*. Retrieved October 4, 2018, from http://www.newindianexpress.com/cities/kochi/2018/oct/07/online-child-sexual-abuse-on-the-rise-1882079.html

UNICEF. (2011). *Child Safety Online : Global challenges.* Retrieved from https://www.unicef-irc.org/publications/pdf/ict_eng.pdf

UNICEF. (2011). *Child Safety Online, Global Strategies and Challenges.* Florence: UNICEF.

UNICEF. (2016). *Child Online Protection.* UNICEF. Retrieved from http://www.icmec.org/wp-content/uploads/2016/09/UNICEF-Child-Protection-Online-India-pub_doc115.pdf

UNICEF. (2017). *Children in a Digital World.* UNICEF.

UNICEF. (2017). *THE STATE OF THE WORLD'S CHILDREN 2017. Children in a Digital World.* New York: UNICEF.

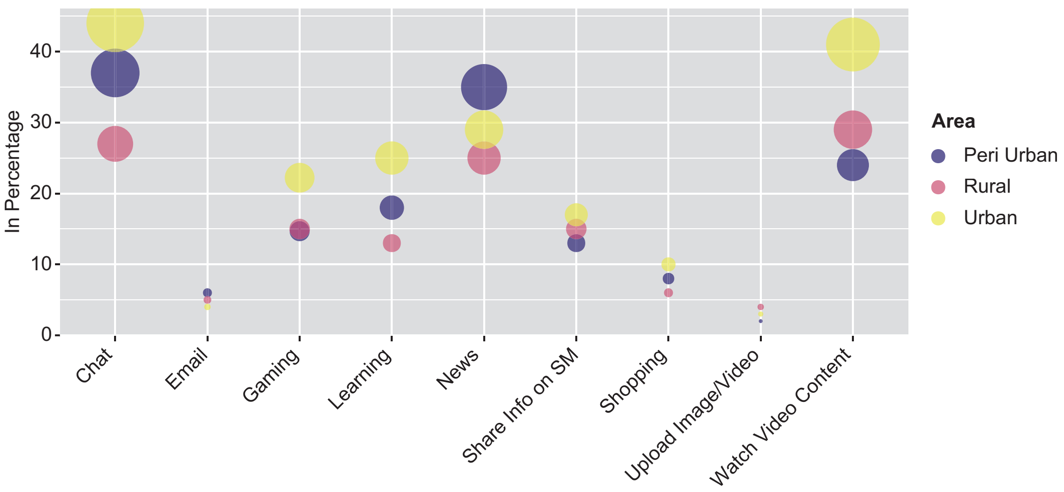
UNODC. (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation.* Vienna: United Nations Office.

Uwe Hasebrink, A. G. (2011). *Patterns of risk and safety online: in-depth analyses from the EU Kids Online survey of 9- to 16-year-olds and their parents in 25 European countries.*

Ybarra, M. L., & Mitchel, K. J. (2008). How Risky Are Social Networking Sites ? : A comparison of places online where youth sexual solicitation and harassment occurs. *Pediatrics, 121*(2).

Part 1 **Annexure:**

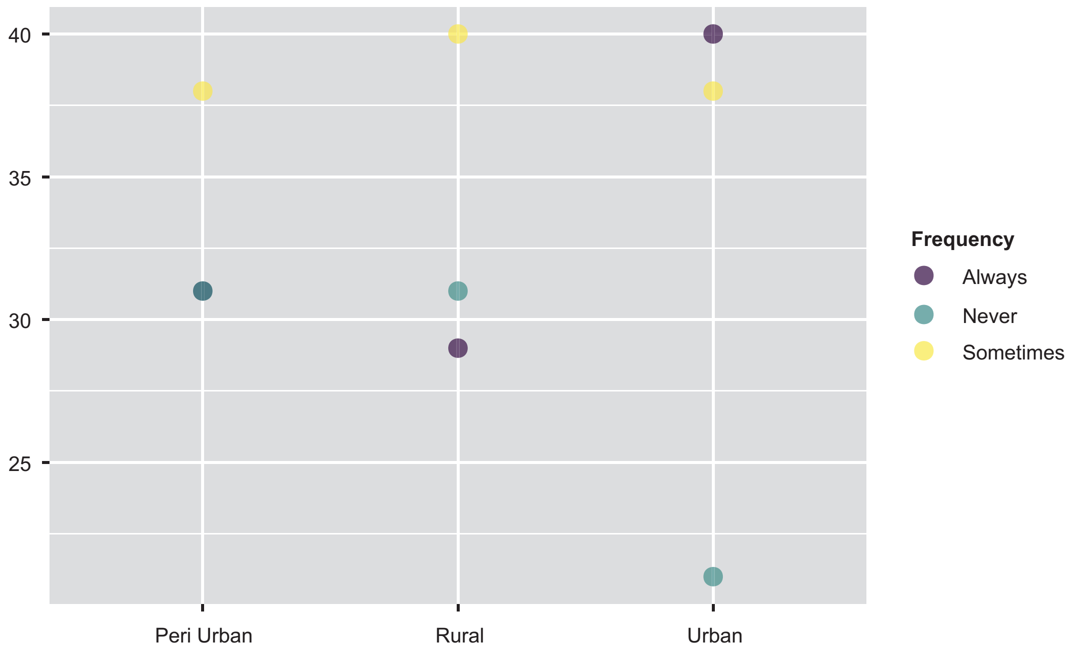
1. Area wise online activities



2. Exposure to inappropriate content by division

Divisions	Insisted to send nudes	Received Inappropriate content	Received Inappropriate text	Sent Inappropriate content	Shared Inappropriate content
Barisal			13%	0%	0%
Chattogram	5%	8%	14%	0%	1%
Dhaka	7%	15%	22%	4%	3%
Khulna	9%	16%	27%	1%	1%
Mymensingh	3%	8%	13%	3%	2%
Rajshahi	7%	16%	25%	2%	2%
Rangpur	2%	13%	18%	1%	0%
Sylhet	4%	14%	21%	1%	0%

3. Guardians' monitoring by area



4. Contact with online acquaintance by age group

Type of Communication	Age Group	Percentage
Voice Chat	10Y-13Y	17%
	14Y-1SY	28%
	16Y-17Y	42%
Video Chat	10Y-13Y	14%
	14Y-1SY	15%
	16Y-17Y	24%
Meet	10Y-13Y	11%
	14Y-15Y	14%
	16Y-17Y	18%

Policy Gap

3.0

Part 2: Policy Gap Mapping

p Mapping

3.0 Part 2: Policy Gap Mapping

3.1 Scope and Approach of the Analysis

In accordance with the rights based approach of United Nations Convention on the Rights of the Child, qualitative legal analysis was conducted on following laws and policies of Bangladesh;

- **Information and Communication Technologies Act 2006**
- **Pornography Control Act (2012)**
- **Digital Security Act (2018)**
- **National ICT Policy of Bangladesh 2018**
- **National Education Policy of Bangladesh 2010**

Along with the legal analysis, concerned country level actors including judges, legal practitioners, child rights activists, NGOs and INGOs, telecom companies and internet service providers were consulted to understand implementation difficulties and the ground level reality. At the final stage, a stakeholder consultation meeting was held to further refine the report and to develop actionable recommendations.

3.1.1 Rights Based Framework to Deal with Online Safety for Children

Given the vulnerability of children, it is essential that they receive enough protection that will allow them to live and develop in a safe and secure environment[13]. However, there is a need to balance this right, with other child

[13] As per Article 19, UNCRC, children have a right to freedom from all sorts of violence - mental or physical. The primary responsibility for ensuring protection of a child is that of the parents of the child, though the state clearly has a relevant role to play in fulfilling various positive and negative obligations - for instance in terms of ensuring appropriate regulation and punishment of offences, appropriate resource allocation, education, health provision etc. In the context of internet safety, this could take the form of protection from unwanted harmful contents or communication in internet, protection from the lack of security that comes from violations of privacy, protection from abuse and bullying etc.

rights recognized by the United Nations Convention on the Rights of the Child (UNCRC).[14]

Moreover, the UDHR[15], ICCPR[16], ICESCR[17], the Constitution of the People's Republic of Bangladesh[18] and the Children Act 2013 also support the rights enshrined in the UNCRC. All these legal instruments have provided a right based framework that can be used to protect children against different kinds of violence and exploitation in internet.

3.1.2 Right to protection from violence, sexual exploitation, and information injurious to their well-being:

No violence is justifiable against a child. Article 19 of UNCRC clarifies that States are required to take all relevant measures to ensure protection of children from violence – mental or physical (thereby including cyberbullying, sexual abuse, etc.). Article 34 of the UNCRC specifically requires children to be protected from sexual abuse and exploitation of all sorts. The Optional Protocol II to the UNCRC particularly emphasizes on the growing availability of harmful contents on the Internet and other evolving technologies that are more vicious in nature. This Optional Protocol II protects children against production, distribution, exportation, transmission, importation, intentional possession and advertising of harmful contents in Internet.[19]

However, this does not mean that a child should always be treated as a victim - instead children should be treated as rights bearing individuals (with no hierarchy between the various rights they enjoy). The protection of children requires a multidisciplinary and coordinated approach to protection requiring cohesive measures being adopted through multiple layers of both government and private sector care givers.[20] Article 7 of the ICCPR recognizes the right to

[14] Notably, the UNCRC does not create a hierarchy of rights with the right to protection at the top. All rights under the UNCRC are given equal weightage and therefore must be appropriately balanced with one another in any given situation.

[15] Universal Declaration of Human Rights, at http://www.un.org/en/universal-declaration-human-rights/, last visited on November 27, 2018.

[16] *International Covenant on Civil and Political Rights*, at https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx, last visited on November 27, 2018.

[17] *International Covenant on Economic, Social and Cultural Rights*, at https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx, last visited on November 27, 2018.

[18] *The Constitution of the People's Republic of Bangladesh*, at http://bdlaws.minlaw.gov.bd/print_sections_all.php?id=367, last visited on November 27, 2018.

[19] See the preamble of *Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography*, at https://www.ohchr.org/en/professionalinterest/pages/opsccrc.aspx, last visited on November 27, 2018.

[20] A 17(e), UNCRC requires states to encourage the development of appropriate guidelines to protect children from information that is injurious to their well-being. This is particularly relevant in the context of the use of ICTs, given the important role of the private sector in regulating the online world.

be free from inhuman or degrading treatment or punishment. Article 9 of the ICESCR ensures the right to social security and Article 10 of ICESCR ensures protection of children from economic and social exploitation. Article 10 of the Constitution of Bangladesh protects a person from any kind of exploitation by another person.

3.1.3 Rights of association, expression, participation, privacy and play

The UNCRC protects a child's rights of expression and identity – notably in Article13[21], 14[22] and 12[23]. Article 15 recognizes children's rights to association and peaceful assembly[24], while Article 16 recognizes that even children have privacy rights[25]. Children also have the right to play, to and engage in recreational activities appropriate to their age.[26] Research on adolescent development suggests that teens have always found ways to explore their sexual identity and express themselves sexually.[27] Freedom of expression and association as well as ensuring appropriate privacy are vital components of ensuring that children grow up as independent, autonomous and functioning social beings.[28]Article 19 of both UDHR and ICCPR recognizes the freedom of the expression of a child. Article 39 of the Constitution of Bangladesh recognizes freedom of thought and conscience, and of speech. In this sense even sexually explicit contents in private intimate chat can be seen as an exercise of these rights and essential to the framing of one's sexual identity. Also, Article 12 of UDHR, Article 17 of the ICCPR and Article 43 of the Constitution of Bangladesh protect children from arbitrary

[21] Which permits limitations only to protection reputations and rights of others; national security, public health, morals and public order.

[22] Which interestingly recognizes that the evolving capacities of a child must be taken into account when providing direction to a child (who is exercising freedom of thought).

[23] Which requires that a child's views be sought and taken into account in all matters affecting him/her and with weightage accorded per the child's maturity.

[24] Which may only be limited in the interests of national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others.

[25] Article 16 requires that children not be subject to unlawful interferences with their privacy or correspondence, and further that they be protected from unlawful attacks on their honor and reputation. This would for instance imply that no disproportionate surveillance be carried out of minors (even to protect them). Exercising the right to private and family life (and data protection) is inherently related to autonomy and self-development of the child.

[26] Article 31, UNCRC.

[27] Implying therefore that unrealistic restrictions are unlikely to be met, and further that adults need to accept children – particularly adolescents - as sexual beings and appropriately advise youngsters on their sexuality. Gillespie, A. "Adolescents, Sexting and Human Rights", 13:4 (2013), *Human Rights Law Review*, pp. 623-643, at p. 626.

[28] An aspect that is often overlooked is the provision of adequate education and training. The UNCRC specifically recognizes the right of children to education in Articles 17, 28 and 29. In today's context this would extend to information about the beneficial uses of technology, potential harms and how to ameliorate the same.

interference with their privacy. So, the personal intimate communication of the children should also be protected from any arbitrary interference and undue influence.

3.1.4 **Consideration of a child's best interests:**

One of the basic principles of the UNCRC is that the best interests of the child must be considered in any decision that affects the child.[29] Accordingly, any limitation of rights of a child must be done keeping in mind the child's best interests. Article 25 of UDHR also talks about the special protection (special care and assistance) of the children. The Article 10 of the ICESCR provides the widest possible protection and assistance to the children. Article 28 of the Constitution of Bangladesh enables the state to create special provisions for the children in order to ensure their best interests.

3.1.5 **Evolving capacities of a child:**

A particularly important principle in the UNCRC is the recognition that children have different capacities and capabilities at different stages of their development.[30] This implies that the needs and requirements of adolescents – with respect to their participation, association, privacy and expression rights must be given greater weightage than those of younger children. Accordingly, legal systems must account for the differences between children of different ages.

3.1.6 **Protection from discrimination:**

The UNCRC is clear in prohibiting discrimination on any basis – be it gender, race, ethnicity or class. Decisions or laws affecting children must be evidence based and not arbitrary in nature. Article 7 of the UDHR declares every person is equal before the law and is entitled without any discrimination to equal protection of the law. Article 4, 20, 24 and 26 of the ICCPR and the Article 2 of the ICESCR protect a person from different kinds of discrimination that are based on race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status etc. Article 10 of the ICESCR particularly protects children against discriminatory treatment. Article 38 of the Constitution of Bangladesh prohibits any discrimination on the ground of religion, race, caste, sex, place of birth or language.

[29] Refer Article 3 of UNCRC. This principle applies at all stages of a child's life and in all aspects - from creating laws, to taking judicial, administrative or other decisions that affect a child.

[30] Refer Articles 5, 14 and 31 of the UNCRC.

3.1.7 **Limitations on Punishment:**

The UNCRC itself contains no bar or prohibition on criminalization of children. However, it does limit the punitive action that can be taken against children for breach of laws.[31] Relevant principles include how imprisonment should be a punishment of last resort (after the adoption of administrative and other types of sanctions), avoidance of capital punishment or life sentences to children and how criminal laws should aim to reintegrate and rehabilitate rather than merely punish.[32] In Bangladesh, the same limitation on capital punishment has been imposed through the *BLAST and another vs. Bangladesh and others ['Shukur Ali' Case]*[33]*.* Article 14 of the ICCPR specifically mentions about the separate trial of the juvenile persons and encourages the rehabilitation of the juvenile persons instead of giving them other forms of punishment. The Children Act 2013 also proposes lesser degree of punishments for the children is he or she commits a criminal offence. However, this lesser degree of punishment is up to the discretion of the trial court and the laws regarding this are a bit broad in scope.

Thus, according to UNCRC, children are entitled to all the rights that the adults do.[34] But lack the maturity and understanding that adulthood brings do not allow the children to enjoy all of those rights without special care and protection arrangements. The UNCRC has proclaimed that childhood is entitled to special care and assistance. The UNCRC also recognizes that "the child, by reason of his physical and mental immaturity, needs special safeguards and care, including appropriate legal protection, before as well as after birth"[35]. Therefore, the law must therefore aim to ensure children develop to be independent and functioning members of society rather than pander to antiquated notions of public morality through punishing innocuous or relatively harmless behavior, and rather than limiting the enjoyment of their rights because mere discriminating them as children. At the same time, it is the also responsibility of the state to ensure

[31] Refer mainly Articles 37 and 40 of the UNCRC.

[32] Interestingly, A 28(2), UNCRC requires that disciplinary measures adopted in schools also respect the child's dignity and other provisions of the UNCRC.

[33] Civil Appeal No. 16 of 2010. In this case, the Appellate Division of the Supreme Court of Bangladesh has reviewed the death penalty of Shukur Ali (a minor of 14 years of age while committing the crime) over the rape and murder of a seven-year old, and reduced it to life in jail. As Shukur Ali was minor while committing the crime, Appellate Division opined that he cannot be given death penalty and cited the principle of UDHR and ICCPR in this regard. See, *Bangladesh Legal Aid Services Trust*, at https://www.blast.org.bd/content/laws/Shukur-Ali-Case-Website-Summary.pdf, last visited on September 9, 2019. See also, *Appellate Division reviews death penalty of Shukur Ali, lowers it to life in prison*, Bdnews24.com, at https://bdnews24.com/bangladesh/2015/08/03/appellate-division-reviews-death-penalty-of-shukur-ali-lowers-it-to-life-in-prison, last visited on September 9, 2018.

[34] The preamble of the UNCRC considers that the child should be fully prepared to live an individual life in society, and brought up in the spirit of the ideals proclaimed in the Charter of the United Nations, and in particular in the spirit of peace, dignity, tolerance, freedom, equality and solidarity.

[35] See the preamble of UNCRC.

that children learn to use ICTs responsibly. Law must recognize the benefits that digital tools can bring to children and at the same time act so as to mitigate harm. In this respect, the necessity, suitability and proportionality of measures taken to limit rights is essential.[36]

3.2 Gaps in the Laws, Policies, and implementation

3.2.1 Loopholes found in the Criminal Laws of Bangladesh

Bangladeshi laws reflect that all people (both adults and children[37]) are generally prohibited from circulating sexual contents of any kind and in virtually any context. Bangladesh has two specific laws, e.g. *Pornography Control Act 2012* and *Children Act 2013* to govern sexually explicit contents that affect children, e.g. prohibiting the creation, possession, or distribution of child pornography. However, the sharing of sexually explicit messages and associated acts (such as coercion, defamation, etc.) can be covered under the *Penal Code 1860*[38] (PC), *The Children Act 2013*[39] (CA), the *Information and Communications Technology Act, 2006*[40] *(ICT Act), Nari-O-Shishu Nirjatan Daman Ain 2000 (The Prevention of Oppression Against Women and Children Act 2000*[41]*)*, and the *Pornography*

[36] Often however we see that disproportionate measures - such as criminalization or complete denial of Internet access - are adopted in the name of child protection. For instance, the DPS MMS incident of 2004 in India (where an explicit video featuring two students from a leading Delhi school went viral) led to the introduction of mobile phone bans in many schools across the country. See generally, Goswami, I., Rani Premkumar, R., "The Ban on Moabile Phones in Schools in India: A Probe to Augment Efficacy in Policy Execution"Vol. 4, Issue 1 (January 2014), *International Journal of Physical and Social Sciences,* at http://www.academia.edu/5586686/The_ban_on_mobile_phones_in_the_schools_in_India_A_probe_to_augment_efficacy_in_policy_execution, last visited on November 27, 2018.

[37] Those under 18 years of age. See the Children's Act 2013 (Act No. XXIV of 2013), at http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=1119, last visited on June 10 2018. Also see the Majority Act, 1875 (Act No. IX of 1875), at http://bdlaws.minlaw.gov.bd/print_sections_all.php?id=33, last visited on November 27, 2018.

[38] Act No. XLV of 1860, at http://bdlaws.minlaw.gov.bd/print_sections_all.php?id=11, last visited on November 27, 2018.

[39] Act No. XXIV of 2013, at http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=1119,last visited on November 27, 2018; see also Ali, I., "The Children Act 2013:A Commentary by Justice Imman Ali", (2013), *Bangladesh Legal Aid Services Trust and Penal Reform International (PRI)*, at https://www.blast.org.bd/content/publications/The-Children-Act%202013.pdf, last visited on November 27, 2018.

[40] See International Center for Not-for-profit Law, at http://www.icnl.org/research/library/files/Bangladesh/comm2006.pdf, last visited on November 27, 2018; Anonymous, "Bangladesh: analysis of Information Communication Technology Act" (April 2016), *Article19*, at https://www.article19.org/data/files/medialibrary/38365/Bangladesh-ICT-Law-Analysis.pdf, last visited on November 27, 2018; Anonymous, "ICT (Amendment) Act, 2013: Right to Information and Freedom of Expression under Threat" (October, 2013), *Ain o Salish Kendra (ASK)*, at http://www.askbd.org/ask/2013/10/09/ict-amendment-act-2013-information-freedom-expression-threat/, last visited on November 27, 2018.

[41] Unofficial translation of POAWC Act, see International Knowledge Network of Women in Politics, at http://iknowpolitics.org/sites/default/files/prevention_act_bangladesh.pdf, last visited on November 27, 2018. The original law in Bengali can be found at http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=835, last visited on November 27, 2018.

Control Act 2012[42] (PC Act). Moreover, the Digital Security Act 2018 has come into play already in addition ICT Act.[43]All these laws apply independent of the age of the perpetrator, though special provisions for prosecution and sentencing of minors are prescribed under the *Children Act 2013*[44].

Moreover, in ***BNWLA vs Government of Bangladesh***[45], the High Court Division banned 'eve teasing'[46] in any form which also covers public sexual harassment including electronic means and bullying online. But these laws are not comprehensive to deal with the online sexual harassment against child which has been elaborated in the following charts and chapters. So, the laws need to be reformed in order to give better protection to the children.

Bangladeshi laws have dealt with the challenge posed by ICTs in one primary way - through criminalization of what is considered harmful behavior. However, the objectives of dealing with the ICT related challenges are completely different from the objectives of dealing with online child abuse. For example, the Penal Code completely misses this aspect as that time there was no internet. ICT Act was mainly created to deal with digital signatures for protection of online business transactions. And although PC Act deals with some aspects of obscene online contents, it is completely silent about personal use of obscene contents which do not carry criminal intent.[47] Also, criminalizing online harassment or harmful behavior online as cybercrime under ICT Act, Pornography Control Act, and the Digital Security Act might have potential problem because cybercrime policy under these laws focus more on the control and security aspect. By focusing so much on control, cybercrime policy risks overlooking the importance of allowing children and adolescents to experiment online, and to learn from possible mistakes they make.

The following tabular representations of ICT Act, Pornography Control Act and the Digital Security Act provides us with the glimpse on the issues that need to be sorted out in order to prevent online harassment against children in Bangladesh. The first column of the table mentions the important issues and

[42] Act No. IX of 2012, at http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=1091, last visited on November 27, 2018.

[43] *Bangladesh: Scrap Draconian Elements of Digital Security Act.* (2018). Human Rights Watch, at https://www.hrw.org/news/2018/02/22/bangladesh-scrap-draconian-elements-digital-security-act, last visited on November 27, 2018.

[44] See Chapter 5 and 6 of the Children Act 2013.

[45] 2011 BLD (HC) 31, *Bangladesh Legal Aid Services Trust*, at https://www.blast.org.bd/content/judgement/BNWLA-VS-Bangladesh2.pdf, last visited on November 27, 2018.

[46] According to this case judgment, 'eve teasing' denotes public sexual harassment, street harassment and molestation of women by men. This also includes bullying online.

[47] Anonymous, "Brave New World, Same Rights: How Gender, Sexuality, and Rights Intersect in the Digital Lives of Women" (December, 2014), *Bangladesh Legal Aid Services Trust*, at https://www.blast.org.bd/content/report/Report-Bishakh-Datta.pdf, last visited on November 27, 2018.

different rights that need to be considered for the prevention of online sexual harassment against children. The second, third and fourth columns mention existing provisions of ICT Act, Pornography control Act and Digital security Act in comparison to the issues mentioned in the first column by indicating loopholes in these laws. The fifth column, along with Part 2 Annexure provides policy recommendations in order to mitigate those loopholes mentioned in previous three columns through comparing or referring to good practices by the international or regional instruments around the world.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
About Definitions				
Cyber bullying				
Grooming	Not defined	Not defined	Not defined	Definition can be taken from the UNODC Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children[48]. Please see the draft definition in Annexure of this paper

[48] *Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children (2014)*. Commission on Crime Prevention , and Criminal Justice, United Nations Office on Drugs and Crime, at https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_23/E-CN15-2014-CRP1_E.pdf, last visited on November 27, 2018.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
Emotional harassment	Not defined	Section 8 (2) partially deals with this matter by criminalizing mental harassment through showing pornography. But it misses other aspects of emotional harassment such as harassment through bullying, defamation, intimidation etc.	Not defined	The emotional harassment shall also be recognized as one of the forms of cyberbullying, thus be inserted in the Digital Security Act 2018 in accordance with the Section 30(2) of the Children Act 2013 which considers the mental condition of children while giving verdict by the Children Court.
Defamation and exposure	Previously defamation and exposure were criminalized in this law, but now it is replaced by the Section 28 and 29 of the Digital Security Act 2018.	Defined by the Section 8(2) of this Act.	Section 28 and 29 clearly criminalizes defamation by exposing harmful contents online.	The trial of any offence regarding defamation and exposure of children online should be in compliance with the perspectives set forth in Section 30 of the Children Act 2013. The Section 30 considers following criteria while giving verdict at the Children Court- age; sex; physical and mental condition; educational qualification; social, cultural and ethnological status; economic

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
				condition of children's family; cause, accomplice, overall situation and context of the crime committed; children's opinion; social investigation report and other necessary conditions necessary for the best interest of children.
Intimidation	Not defined	Partially defined in Section 8(1) and section 8(2). If a person compels a child to engage in pornographic content making or production, the person will be punished with imprisonment and fine under Section 8(1). So, if it is done with intimidation, it might fall under this section. If it is done with intimidation for defaming a person, it will fall under Section 8(2)	Section 25 criminalizes the intimidation to any person in digital medium.	

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
Social Exclusion	Not defined	Not defined	Not defined	The National ICT Policy of 2018 shall cover this aspect as a policy framework in order to ensure inclusive internet. The government can take the approach of empowering and promoting the social, economic and political inclusion of all, irrespective of age and sex which are set forth in the Goal 10.2 of the Sustainable Development Goals (SDGs)[49].
Online sexual abuse				
Sexual harassment	Not defined	Not defined	Not defined	The definition of online sexual harassment should be drafted and be inserted in the PC Act. The ICT Act and Digital Security Act (DS Act) shall follow the PC Act.

[49] Goal 10, *Sustainable Development Goals*, at https://sustainabledevelopment.un.org/sdg10, last visited on January 15, 2019.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
				While drafting the definition, ideas can be taken from the principles of the DIRECTIVE 2011/92/EU[50] and also from the U.S. National Library of Medicine.[51] Please see the draft definition in Annexure of this paper
Sexual solicitation, also aggressive	Not defined	Partially defined as Section 8(2) criminalizes the seduction of a child to engage into sexual activities.	Not defined	Shall be criminalized in accordance with the Section 28 which says public morality shall be protected.
Blackmail and financial extortion	Not defined	Not defined	Not defined	Definition of "Sextortion" can be taken from Luxemburg Guideline[52] Please see the draft definition in Annexure of this paper

[50] *DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093, last visited on November 27, 2018.

[51] *Medline Plus (2008)*. U.S. National Library of Medicine, at https://medlineplus.gov/childsexualabuse.html, last visited on November 27, 2018.

[52] *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, at http://luxembourgguidelines.org/, last visited on November 27, 2018.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
Online sexual exploitation				
Production and consumption of child sexual abuse materials	Absent	Definition of Pornography (S. 2) and Definition of Child Pornography (S. 8) is there	Absent	Definition can be taken from the DIRECTIVE 2011/92/EU[53] to make the existing provisions more comprehensive. Please see the draft definition in Annexure of this paper
Sexual solicitation, also aggressive	Not defined	Not defined	Not defined	Definition can be taken from the UNODC Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children[54]. Please see the draft definition in Annexure of this paper
Commercial sexual exploitation and trafficking	Not defined	Commercial sexual exploitation is criminalized in Section 8(5) and Section 8(6).	Not defined	Actions should include coordinating more closely at the international and national levels

[53] *DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093, last visited on November 27, 2018.

[54] *Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children (2014)*. Commission on Crime Prevention , and Criminal Justice, United Nations Office on Drugs and Crime, at https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_23/E-CN15-2014-CRP1_E.pdf, last visited on November 27, 2018.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
		Trafficking has not been defined.		and deepening collaboration between law enforcement and the technology industry to keep pace with digital technology that can enable and conceal illegal trafficking and other online child sexual abuse.[55]
Cyber radicalization				
Ideological indoctrination and recruitment	Not Defined	Not defined	Can be tried under Section 27 and 31 if the objective of indoctrination and recruitment is for sedition, deteriorating law and order situation, creating fear among people in the society, spreading terror etc.	Section 6 of the Anti-Terrorism Act 2009 comes into play here if this indoctrination leads to spreading terrorism and committing organized crimes. Also, the National ICT policy 2018 should promote the Goal 16.4 and 16.A of SDGs in order to prevent violence and combat terrorism and crime[56].

[55] The State of the World's Children 2017: Children in a Digital World (2017). UNICEF, at https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, last visited on January 17, 2019.

[56] Goal 16, *Sustainable Development Goals*, at https://sustainabledevelopment.un.org/sdg16, last visited on January 15, 2019.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
Threats or acts of extreme violence	Not defined	Not defined	Can be tried under Section 27 and 31 if it leads to sedition, deteriorating law and order situation, creating fear among people in the society, spreading terror etc.	Section 6 of the Anti-Terrorism Act 2009 comes into play here if this extreme violence leads to spreading terrorism and committing organized crimes. Also, the National ICT policy 2018 should promote the Goal 16.4 and 16.A of SDGs in order to prevent violence and combat terrorism and crime[57].
Online attacks and frauds				
Attack on devices: malware infection	Not defined	Not defined	Criminalized in Section 19 of this Act	
Exposure to inappropriate content: Pharming	Not defined	Criminalized in section 8(4), 8(5) of this Act.	Criminalized in Section 27 as it is a kind of cyber-attack. It is also indirectly or partially criminalized under Section 28 and 29 of this Act is this pharming goes against public morality and defames concerned persons.	

[57] Goal 16, *Sustainable Development Goals*, at https://sustainabledevelopment.un.org/sdg16, last visited on January 15, 2019.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
Identity theft: phishing, hacking, privacy breach	Privacy breach is criminalized in Section 63.	Not defined	Phishing is criminalized in Section 26. Hacking is criminalized in Section 34. Privacy breach is criminalized in Section 26 and 33.	
Malvertising	Not defined	Criminalized in section 8(3), 8(4) of this Act.	Criminalized in Section 19 of this Act.	
Production and consumption of pirated music and videos	Not defined	Not defined	Not defined. Partially can be criminalized under Section 22 (digital forgery) and Section 23 (Digital fraud)	
Online enticement				
Harmful behaviour: exposure to inappropriate content, access to alcohol and drugs	Not defined	Exposure to inappropriate content is criminalized in Section 8(4) and 8(6). Nothing is said about access to alcohol and drugs.	Not defined. Can be criminalized partially if exposure to inappropriate content leads to deterioration of public law and order situation under Section 31	

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
Illegal behaviour: cheating, plagiarism, gambling, drug trafficking	Not defined	Not defined	Not defined. Can be criminalized partially if plagiarism, gambling, drug trafficking lead to deterioration of public law and order situation under Section 31 Cheating can be criminalized partially if it is related to digital forgery (Section 22) and digital fraud (Section 23) Also cheating by impersonation is criminalized under Section 24.	
Self-harm: sexting, self-exposure	Not defined	Is criminalized under Section 8(4) if creates public nuisance.	Is criminalized under Section 28 as it hurts the religious sentiment and against the public morality.	
Other risks				
Enticement for drug trafficking	Not defined	Not defined	Not defined	
Financial fraud	Not defined. Can be criminalized partially if financial fraud is done through false electronic certificate.	Not defined	Unauthorized e-transaction is criminalized under Section 30. Can also be criminalized is done through digital forgery (Section 22) and digital fraud (Section 23)	

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
Definition of Cyber harassment, cyberbullying and cyber stalking	Not defined	Not defined	Not Defined	Definition should be drafted and the example can be taken from the Luxemburg Guideline[58] and also from the UNODC Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children.[59] Please see the draft definition in Annexure of this paper These definitions should be inserted in Chapter II (General Explanations) of the Penal Code, 1860
Definition of Child	Not defined	Section 2(e) of the PC Act refers the Children Act 1974 which is now replaced by the Children Act 2013	Not Defined	Section 4 of the Children Act 2013 prevails all these laws and recognizes anyone below 18 years of age as a child. The author suggests to take the definition of Children Act 2013 for granted as it complies with UNCRC.

[58] *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, at http://luxembourgguidelines.org/, last visited on November 27, 2018.

[59] Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children (2015). United Nations Office on Drugs and Crime, at http://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf, last visited on November 27, 2018.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
Definition of Cybercrime	Not Defined However, damage to computer system (S. 54), change of computer source code (S. 55), computer hacking (S. 56), circulation of false, obscene and defamatory statement (S. 57), Unauthorized and illegal access into a protected computer system (S. 61), impersonification and concealment of facts (S. 62), breach of privacy (S. 63), false electronic signature (S. 64), use of electronic signature for fraud (S. 65) have been criminalized	Not defined	Not Defined However, Digital Forgery (S. 22), Digital/ Electronic Fraud (S. 23), Cyber-terrorism (S. 27), Hate speech against religion or values (S. 28), Defamation online (S. 29), Computer/ Digital-espionage (S.32), Computer Hacking (S. 34) either have been defined or criminalized	Definition should be drafted in compliance with the Article 2 to Article 11 of the Convention on Cybercrime 2001 (Budapest Convention) for the comprehensive definition of cybercrime. According to the Budapest Convention, the definition of cybercrime can be following[60]: i) offences against the confidentiality, integrity and availability of computer data and systems; ii) computer-related offences; iii) content-related offences; iv) offences related to infringements of copyright and related rights. Please see the draft definition in Annexure of this paper

[60] *Cybercrime: Global Programme on Cybercrime*, United Nations office on Drugs and Crimes, at http://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html, last visited on November 27, 2018.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
Definition of sextortion	Not defined	Not defined	Not defined	Definition can be taken from Luxemburg Guideline[61] Please see the draft definition in Annexure of this paper
Definition of Digital Evidence and digital foot print	Not defined	Not defined	Not defined	The definition can be drafted in aligned with the European Commission's science and knowledge service[62] Please see the draft definition in Annexure of this paper
Definition of Child Pornography	Absent	Definition of Pornography (S. 2) and Definition of Child Pornography (S. 8)	Absent	Definition can be taken from the DIRECTIVE 2011/92/EU[63] to make the existing provisions more comprehensive. Please see the draft definition in Annexure of this paper

[61] *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, at http://luxembourgguidelines.org/, last visited on November 27, 2018.

[62] *Digital footprint, Dictionary.com*, at https://www.dictionary.com/browse/digital-footprint, last visited on November 27, 2018. See also, Digital Footprints: Online identity management and search in the age of transparency (2007), pp. 3-4 Pew Internet, at http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP_Digital_Footprints.pdf.pdf, last visited on September 9 2018.

[63] *DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093, last visited on November 27, 2018.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
About Justice Administration				
Provision of separate Juvenile Court to try child victim or child accused	Not recognized	Not Recognized	Not recognized	The provision for the Juvenile court under Section 16 to Section 43 of the children Act shall prevail all these laws. Any matter involving "Children in Conflict with the Law"[64] and "Children in Contact with the Law"[65] shall be tried in separate juvenile court.
Provision for Cyber Tribunal	Provision for Cyber Tribunal (S. 68-81) and Cyber Appellate Tribunal (S. 82-84). Applicable both for adult and children.	No provision	Refers to the ICT Act for Cyber Tribunal and Cyber Appellate Tribunal (S. 2). Applicable both for adult and children.	Any matter involving "Children in Conflict with the Law"[66] and "Children in Contact with the Law"[67] shall be tried in separate juvenile court instead of trying them in Cyber Tribunal
Provision for camera trial for a child victim (Children in Contact with the Law" or accused (Children in conflict with the law)	Absent	Absent	Absent	Privacy of the child victim of accused shall be maintained according to the Section 28 of the Children Act.

[64] Section 2(3) of the Children Act 2013.

[65] Section 2(4) of the Children Act 2013.

[66] Section 2(3) of the Children Act 2013.

[67] Section 2(4) of the Children Act 2013.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
Summary Trial for the Cybercrime committed by a child or for a child victim	Absent	Absent	Absent	The Section 32 of Children Act 2013 imposes 360 days' time limitation for completing trial in juvenile court. This time frame has to be reduced in according with the United Nations Standard Minimum Rules for the Administration of Juvenile Justice ("The Beijing Rules")[68] can be followed here.
Diversion or other alternative initiatives to the classical criminal justice systems to avoid recourse to the criminal justice systems for young persons accused of an offence	Absent	Absent	Absent	Section 30. 31, 33, 34, 48, 49, 50, 51 and 54 of the Children Act 2013 provide a broad range of alternative and educative measures at the pre-arrest, pre-trial, trial and post-trial stages, in order to prevent recidivism and promote the social rehabilitation of child offenders. This can be improved in accordance with the UNODC Guidelines for Action on Children in the Criminal Justice System[69].

[68] *The Beijing Rules* (1985). United Nations Standard Minimum Rules for the Administration of Juvenile Justice, at http://www.unodc.org/pdf/criminal_justice/UN_Standard_Minimum_Rules_for_the_Admin_of_Juvenile_Justice_Beijing_Rules.pdf. Last visited on November 27, 2018.

[69] Guidelines for Action on Children in the Criminal Justice System (1997). United Nations Office of the Drugs and Crimes. At http://www.unodc.org/pdf/criminal_justice/Guidelines_for_Action_on_Children_in_the_Criminal_Justice_System.pdf, last visited on November 27, 2018.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
About Investigation of Online Harassment				
Provision for Digital Security Agency	Not clear. Regulatory and certificate issuing authority (S. 18-19) is there. Recognition of foreign regulatory authority is recognized (S. 20).	Not defined	Yes. Provision for Digital Security Agency (S. 5-7). Provisions for CERT (S. 9). Digital Security Council (S. 12-14)	
Characteristics of the Digital Security Authority	Administrative. Not judicial or quasi-judicial	Not defined	Administrative. Not judicial or quasi-judicial	Introduction of Cyber Emergency Response Team (CERT) can serve the purpose of a Digital Security Authority. This specialized body should be made quasi-judicial in nature including law enforcement personnel, judicial officers, technical experts, legal practitioners and members of the civil society. Our proposal is to make this body as a "One Stop Service Canter" from where the child victim and offender can get all the specialized treatments of juvenile justice.

Topic/ Issue	Information and Communications Technology Act 2006	Pornography Control Act 2012	Digital Security Act 2018	Recommendations for Criminal Laws of Bangladesh
Provision for Digital Forensic Lab	No provision	No provision	Provision for Digital Forensic Lab is there in Section 10-11, but a detailed "rules and regulations" are yet to be prescribed to make these sections effective	
Provision for the specialized training of the law enforcement personnel, judicial officers, legal practitioners and other concerned government officers.	No provision	No provision	Section 13(2) partially talks about the policy making for specialized training by the Digital Security Council.	Specific provisions on providing specialized training to deal with cases where victim (Children in Contact with the Law" or accused (Children in conflict with the law) are concerned. These training include regular training of the law enforcement agencies, judicial officers, public prosecutors and other concerned government officials. Moreover, a specialized body called 'Cyber Police" can be introduced to meet this demand. The relevant provisions can be drawn from Lanzarote Convention of the Council of Europe[70].

[70] Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007). Council of Europe, at https://rm.coe.int/1680470937, last visited on November 27, 2018.

3.2.2 Loopholes found in the National Information and Communication Technology Policy 2018 and National Education Policy 2010 of Bangladesh

The National Information and Communication Technology Policy 2018[71] (The ICT Policy) and the National Education Policy 2010[72] are two important policy guidelines to ensure internet safety of the children in Bangladesh. The following are the brief on these two policies-

i. National ICT Policy 2018

The National ICT Policy contains specific provisions in second and third chapters regarding protection of children in online. In second chapter, one of the objectives of this ICT Policy is set out as ensuring Digital Security[73]. Under this, the government of Bangladesh sets its objective for ensuring safe and risk-free usage of ICT. In detailed action plan at ANNEX I of the ICT Policy 2018, the government relies on BTRC to ensure safe usage of internet as a short-term plan to be achieved by 2021[74]. In Action Plan No. 2.2.2, Ministry of Law, Justice and Parliamentary Affairs, Ministry of Public Administration and the Public Safety Department of Bangladesh Police are entrusted with organizing training program on internet safety for the judicial officers, legal practitioners, enforcement agencies and other concerned experts as a short-term plan to be achieved by 2021. The ICT Ministry is liable for creating a central platform to strengthen the capacity of CIRT, creating instant live reporting mechanism and building public awareness under action plan 2.2.3. ICT Ministry is also liable for creating a poll of cyber security experts under action plan 2.2.3. And the Cabinet Division of the government, Ministry of Public Administration and ICT Ministry is jointly liable to appoint safety focal officers in all concerned government ministries. The problem with all of these policies is that they are to be achieved as a short-term basis by 2021. But these goals should be long term goals by the government because the safety measures of the internet are rapidly and consistently being changed. That is why these are mandatory priorities on a regular basis.

[71] National Information and Communication Technology Policy 2018, at https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/policies/0b508068_d74f_45a1_864a_516536af3060/National%20ICT%20Policy.pdf, last visited on December 22, 2018

[72] National Education Policy 2010, at http://old.moedu.gov.bd/index.php?option=com_content&task=view&id=338&Itemid=416, last visited on December 22, 2018

[73] Policy no. 2.2.2, See National Information and Communication Technology Policy 2018, p. 15, at https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/policies/0b508068_d74f_45a1_864a_516536af3060/National%20ICT%20Policy.pdf, last visited on December 22, 2018

[74] Action plan no. 2.2.1, See National Information and Communication Technology Policy 2018, p. 30, at https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/policies/0b508068_d74f_45a1_864a_516536af3060/National%20ICT%20Policy.pdf, last visited on December 22, 2018

The Policy no. 3.2.4 specially talk about protection women and children from the unwanted and harmful contents in social media as well as in any digital medium. The policy no 3.2.5 urges the state to take necessary steps for prevention and mitigation of digital crimes. The Action Plan no. 2.4 deals with Policy No. 3.2.4 and 3.2.5 in detailed, The Action plan No. 2.4 emphasizes on creation of a cell which will monitor and analyze the data in order to prevent and mitigate unwanted and harmful contents in social media, and will prescribe safety measures accordingly. The Action plan 2.4.2 engages Department of Secondary and Higher Education, Department of Madrasa and Vocational Education, Ministry of Women and Children Affairs and ICT Ministry to create awareness among the guardians of children so that they can be aware of harmful contents in internet. The action plan 2.4.3 empowers BTRC and Ministry of Women and Children Affairs to block harmful contents in internet. However, all these actions are also for short term which is to be achieved by 2021. Therefore, government should also extend these actions plans to mid-term (to be achieved by 2030) and long-term (to be achieved by 2041) plans.

ii. National Education Policy 2010

The National Education Policy 2010 emphasizes on educating every child in Bangladesh. This serves as the fundamental basis of creating awareness on internet safety among children in Bangladesh. In Chapter 1 government gives importance on ICT education for creating a knowledge based society in Goal 12. The Chapter 12 of Education Policy talks about ICT education and chapter 26 talks about curriculum development. In Chapter 12, the Education Policy is silent on creating awareness on internet safety, especially for women and children. All the Education Policy talks about is computer literacy, training on technical aspects of ICT and reforming higher education to create technical experts on ICT. But it misses the whole debate of internet safety and other online associated risks. The Chapter 26 does not mention about developing updated curriculum on ICT education. It generally talks about curriculum development, review of existing curriculum on the text books of primary, secondary and higher secondary education, and talks about publication of text books also. But a comprehensive curriculum development on ICT education including curriculum on internet safety is missing here.

3.3 Recommendations

I. The Digital Security Act, the Information and Communications Technology Act, the Pornography Control Act and National ICT Policy 2018 should contain special chapter for the protection of children online. As clearly stated in previous chapters that the criminal laws of Bangladesh that are dealing with the violence against children do not contain many important definitions of different types of cybercrime or online harassments. Therefore, new definitions should be inserted in the Digital Security Act, Information and Communications Technology Act and Pornography Control Act.

II. Bangladesh also needs to enact a Personal Data Protection Act in order to protect very sensitive personal data of the children in compliance with international or other regional legal instruments. In this regard, the recently enacted General Data Protection Regulation (GDPR) of the European Union could be a good guiding principle for Bangladesh to be followed as a model law.

III. Most of the Bangladeshi laws that deal with the harassment against children have been made keeping offline perspectives into consideration and they completely miss the online perspectives, for example- the Evidence Act 1872 or the Nari-O-Shishu Nirjatan Daman Ain 2000. That is why these laws are obsolete in order to fight against online violence and harassments. Either Bangladesh needs to enact new law like “Online Harassment Prevention Act” or the existing laws should be reformed where new chapter on “online harassment” will be inserted or the provisions of these laws will also be made applicable for online harassments or abuses also.

IV. Personal and intimate communication between peers or between persons who are in intimate relationship should not be criminalized or penalized in the criminal laws of Bangladesh. Rather the laws should differentiate between conduct out of intimate relationship and conduct due to criminal intention that harm others.

V. There are discrepancies in the Digital Security Act, Information and Communications Technology Act and the Pornography Control Act while imposing punishment and penalty. All these laws grossly impose same punishment both for the child offender and adult offender which is the clear violation of the UNCRC. In this regard, the provisions of the Children Act 2013 shall be made mandatory if an offender or perpetrator is child. The ICT Act and the Digital Security Act must contain lesser degree of punishment to a child offender or perpetrator in compliance with the Children Act 2013 and UNCRC.

VI. Bangladesh shall ratify Budapest Convention (Cybercrime Convention). Also, Bangladesh should incorporate the principles of Lanzarote Convention of the Council of Europe and General Data Protection Regulation (GDPR) of European Union in its domestic laws. It will have following benefits- (a) cooperation in cross border crime prevention, (b) better digital evidence management among laws enforcement agencies, (c) Incorporation of internationally accepted legal definitions However, one of the interviewees of KII has opined that before ratifying international legal and policy instruments, Bangladesh needs to develop frameworks to coordinate among different government agencies so that the underlying principles of international legal and policy instruments can be incorporated into actions plans of these concerned government agencies.

VII. Although the Children Act 2013 compels us to deal cases on online harassment against children at the Children Court, this court is not a specialized court like Cyber Tribunal to deal with the cybercrimes or online based crimes. So, there should be a Cyber Tribunal established in each District Court and the same Cyber Tribunal can be converted to Children Court if the victim or perpetrator of online harassment is a child. Moreover, right now only a District Judge can form and sit in the Cyber Tribunal. So, Joint District Judges should also be allowed to form Children Court to ease the burden from District Judges.

VIII. The arrest of "children in conflict with law" is often done mostly according to the manner of Code of Criminal Procedure. Still the police stations all around the Bangladesh do not have special arrangements for children in accordance with the Children Act.

IX. Specialized cyber police unit needs to be set up in each division of the country.

X. There should be one stop service from government where victims can get technical, legal and law enforcement services. Different agencies and organizations like BTRC, CID Police, RAB, Legal Aid Office of the District Courts, Human Rights organizations should be brought under one umbrella to form a specialized boy. The example of this specialized body can be formation of a Cyber Emergency Response Team (CERT) which is mentioned in the Digital Security Act. The nature of CERT should be qasi-judicial and it should follow less formal procedures in order to give quick response to the victims of online sexual harassment. This CERT can also be a sustainable and way of Alternative Dispute Resolution (ADR) in case of petty online harassments. For grievous nature of online crimes, this CERT will act as a full-fledged trial court having fewer formalities.

XI. There should be anti-harassment committee formed or activated (if there is already) in each educational institution according to the High Court Directives on the case filed by BNWLA. The committee in each educational institution should be made accessible both online offline (hotline or dedicated number). The committee will receive complain from the students or parents of an educational institution, inquire into the matter and impose punishments against the perpetrator of online or offline harassment. The committee will also conduct regular counselling with the students. This could be an alternative good strategy to prevent online harassment against children.

XII. A national team taskforce should be made, where all the stakeholders will work together to ensure safe internet use.

XIII. In order to encourage proper use of media, more child friendly content should be developed focusing on; (a) drawing children attention and interest. And (b) reflecting the history and culture of our country so that the children get the opportunity to learn about Bangladesh.

XIV. Not all content which are appropriate for adults are suitable for children, hence, identifying and filtering these content is important for child protection. Since, telecom companies and Internet Service Providers have very important responsibility to block availability of such content to children, government should develop some form of guidebook for these organizations. The guidebook should be made after thorough research, and strong institutional mechanism should be developed for ensuring compliance.

XV. The ICT curriculum at the Secondary level should incorporate ethical and social use of ICT. Since, children are getting access to Internet at increasingly earlier ages, ICT education should be made compulsory at the Primary level incorporating content on internet safety. However, school-based campaign or inclusion of internet safety related materials in the curricula will not be effective to create awareness or develop safety skills of non-school going children. Hence, developing specialized content and reaching out to them via alternative channels are essential

XVI. There is a growing concerns about device dependency among children as young as one year old. Interviews with the stakeholders revealed cases of digital dependency among toddlers affecting their mental development. In order gain comprehensive understanding of prevalence of digital dependency and their potential impact, large scale study is required to avert the potential health crisis.

Part 2 **Bibliography**

(a) Primary (Treaties, Legislation, Policy Documents, Case Laws):

1) *BNWLA vs Government of Bangladesh*, 2011 BLD (HC) 31, the High Court Division of the Supreme Court of Bangladesh banned 'eve teasing'.

2) *Karttunen* v. *Finland*, European Court of Human Rights, Application no. 1685/10, May 10, 2011.

3) Marta Santos Pais, "Annual Report of the Special Representative of the Secretary General on Violence Against Children", *Human Rights Council, United Nations General Assembly*, January 5, 2016, A/HRC/31/20.

4) *Matthew* v. *Harris*, 2017 Cal. App. LEXIS 9.

5) Office of the High Commissioner, Human Rights, "New Digital Technologies Produce Unprecedented Levels of Child Abuse Material Online", *United Nations High Commissioner on Human Rights*, March 28, 2016.

6) *R.* v. *John Robin Sharpe*, [2001] 1 SCR 45.

7) Rashida Manjoo, "Report of the UN Special Rapporteur on Violence Against Women", *Human Rights Council, United Nations General Assembly,* May 19, 2015, A/HRC/29/27/Add.2.

8) "Recommendation CM/REC (2017)x of the Committee of Ministers to Member States on [Comprehensive] Guidelines to empower, protect and support children's [safe access to their rights on the Internet] [rights in the digital environment] (first draft, 20 March 2017)", Ad Hoc Committee For the Rights of the Child, Council of Europe, Strasbourg, March 20, 2017, privately circulated.

9) The Children's Act, 2013.

10) The Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, 2007.

11) The Digital Security Act, 2016 (proposed).

12) The Information and Communications Technology Act, 2006.

13) The Penal Code, 1860.

14) The Pornography Control Act, 2012.

15) The Prevention of Oppression Against Women and Children Act, 2000.

16) "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse", *Adopted by the Interagency Working Group in Luxembourg*, January 28, 2016.

17) United Nations Convention on the Rights of the Child, 1989.

(b) Secondary (Articles, Books, Reports):

1) Alisdair A. Gillespie, "Adolescents, Sexting and Human Rights", *Human Rights Law Review*, 13:4 (2013), pp. 623-643.

2) Amelia Abraham and Christina Kenny, "Is it right to criminalize children who share sexts?", *The Guardian,* July 26, 2014.

3) Anita Gurumurthy et. al., "Technology Mediated Violence Against Women in India: How Can we Strengthen Existing Legal Institutional Response Mechanisms", *IT For Change,* January 2017.

4) Anonymous, "The Criminalization of Youth", *Pacific Standard,* March 17, 2015.

5) Anonymous, "Distribution of Facebook Users Worldwide as of January 2017, by age and gender", *Statista*.

6) Anonymous, "Number of Monthly Active WhatsApp users worldwide", *Statista*.

7) Anonymous, "Selfies: Protecting Young People Online…from themselves?", Internet Watch Foundation.

8) Anonymous, "Sexting Teens Criminalized as Sex Offenders", *Child Rights International Network*, CRIN Mail 1472, May 6, 2015.

9) Anonymous, "Teenage Sexting Statistics", *GuardChild,* April 2017, available at https://www.guardchild.com/teenage-sexting-statistics/.

10) Anonymous, "United Kingdom: Sexting Boy's Naked Selfie Recorded as a Crime by Police", *Child Rights International Network*, September 7, 2015.

11) Anonymous, "Watching porn in public can't come under freedom of speech: SC seeks means to curb child pornography", *FirstPost*, February 27, 2016.

12) Anonymous, "Why The Criminalization of Consensual Sexual Exploration BetweenTeenagers is Unconstitutional", *Constitutionally Speaking,* January 17, 2013.

13) Anthony Zurcher, "Teen Sexting Prosecution Sparks Outrage", *BBC News,* July 10, 2014.

14) Arafatul Islam, "More Bangladeshi girls harassed online than ever", *Deutsche Welle*, April 19, 2017.

15) "Brave New World, Same Rights: How Gender, Sexuality, and Rights Intersect in the Digital Lives of Women", *Bangladesh Legal Aid Services Trust (BLAST)*, December 3, 2014.

16) Centre for Justice and Crime Prevention South Africa, "Digital Media and Child Rights: Submission on Day of General Discussion", *United Nations Committee on the Rights of the Child*, September 12, 2014, Geneva.

17) "Child Online Protection in India", *UNICEF*, New Delhi, 2016.

18) Christina Nomdo, "Criminalizing Consensual Sexual Activities of Adolescents in South Africa", *Article 40*, Volume16, Issue 1, June 2014.

19) Damien Gayle, "Sexting Could See Teenagers Branded as Sex Offenders", *The Guardian,* May 4, 2015.

20) Danah Boyd, *It's Complicated: The social lives of networked teens*, Yale University Press, 2014.

21) Desh Kapoor, "How To Deal With MMS Scandals and the Consequent Situations", *Drishti*, October 2016.

22) Draft version of the "Digital Security Act, 2016" (2016), *Forum Asia*, March 9, 2016.

23) ECPAT, "Briefing Note to the Committee on the Rights of the Child, Day of General Discussion, 2014, Media, Social Networks and the Rights of the Child", *ECPAT International*, September 2014.

24) EPCAT Global Monitoring Report on the status of action against commercial sexual exploitation. (2006).

25) EreshOmar Jamal, MoyukhMahtab and ShamsuddozaSajen, "Digital Security Act, 2016: How does it affect freedom of expression and the right to dissent?", *The Daily Star*, October 29, 2016.

26) Farzana Hussain, “To Tolerate or Not: Sexual harassment and the law”, *the Independent*. November 25, 2016.

27) Sagar Deshmukh, “Analysis of WhatsApp Users and its usage worldwide”, *International Journal of Scientific and Research Publications*, Volume 5, Issue 8, August 2015.

28) Samantha Payne, “New Mexico Legalises Sexiting Between Two Consenting Teens”, *International Business Times,* February 28, 2016.

29) Senior Correspondent, “73 percent women subject to cyber-crime in Bangladesh”, *bdnews24*, March 9, 2017.

30) Simone van der Hof, Bert-JaapKoops, “Adolescents and Cybercrime - Navigating between freedom and control”, *Policy & Internet*, 2011.

31) Sonia Livingstone, John Carr, Jasmina Byrne, “One in Three: Internet Governance and Child Rights”, *Global Commission on Internet Governance*, November 2015.

32) Staff Correspondent, Anonymous, “Draft Digital Security Act gets green light”, *The Daily Star*, August 23, 2016.

33) Sushmita S. Preetha, “Digital Sexual Harassment in Digital Bangladesh”, *Dhaka Tribune*, May 16, 2015.

Part 2 Annexure:

These definitions have been drafted in aligned with the different regional and international instruments or principle that can be used as reference to reform existing Bangladeshi criminal laws on prevention of online sexual harassment against children

1. Application software (Apps)[75] = A computer programme designed to carry out a specialized task or tasks for the user, such as database management, word processing or electronic mail. A mobile app is software designed to run on mobile devices.

2. Banner advertising[76] = A popular form of website advertising utilizing a rectangular graphic display that stretches across the top or bottom of a website or down the right or left sidebar and when clicked on, directs the user to the website of the advertiser.

3. Child: Any person under 18 years of age.

4. Child Pornography: It consists of images of child sexual abuse, and other particularly serious forms of sexual abuse and sexual exploitation of children through the use of new technologies and the Internet. It includes images recording the sexual abuse of children by adults. It may also include images of children involved in sexually explicit conduct, or of their sexual organs, where such images are produced or used for primarily sexual purposes and exploited with or without the child's knowledge. Furthermore, the concept of child pornography also covers realistic images of a child, where a child is engaged or depicted as being engaged in sexually explicit conduct for primarily sexual purposes.

[75] Supra note 93.

[76] Supra note 93.

5. Child sexual abuse: Also called child molestation, is a form of child abuse in which an adult or older adolescent uses a child for sexual stimulation.

6. Child sex tourism/ travelling child abusers[77] = Child sex tourism is a form of commercial sexual exploitation of children by men or women who travel from one place to another, and there engage in sexual acts with children.

7. Cyberbullying: The use of ICTs to harm a victim or victims in deliberate, repeated and hostile ways and eased by the apparent anonymity and distance from the victim.[78]

8. Cybercrime: According to the Cybercrime Convention (Budapest Convention, the definition of cybercrime is- i) offences against the confidentiality, integrity and availability of computer data and systems; ii) computer-related offences; iii) content-related offences; iv) offences related to infringements of copyright and related rights.[79]

9. Cyber-enticement[80] = The use of a computer or similar device to contact a person who is or is believed to be a minor to solicit, encourage, entice, or lure him or her for the purposes of engaging in sexual activity in violation of the law.

10. Cyber harassment: The use of ICTs to intimidate, repeatedly or otherwise, one individual by another or by a group.[81]

11. Cyber stalking: The use of ICTs to undertake activities related to locating, surveying, harassing or manipulating victims that causes distress, fear or alarm, being mainly characterized by the repetitive aspect of the conduct.[82]

12. Dark net[83] = Part of the deep web in which both web users and website publishers are largely anonymous due to obfuscation technology.

[77] Supra note 93.

[78] Ibid.

[79] *Cybercrime: Global Programme on Cybercrime*, United Nations office on Drugs and Crimes, at http://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html, last visited on November 27, 2018.

[80] Supra note 93.

[81] Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children (2015). United Nations Office on Drugs and Crime, at http://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf, last visited on November 27, 2018.

[82] Supra note 88.

[83] Supra note 93.

13. Deep web[84] = All parts of the internet which cannot be indexed by search engines.

14. Digital Footprint: One's unique set of digital activities, actions, and communications that leave a data trace on the Internet or on a computer or other digital device and can identify the particular user or device.[85] The digital footprint can be classified into two categories[86]:

i. Passive Digital Footprint: Personal data made accessible online with no deliberate intervention from an individual.

ii: Active Digital Footprint: Personal data made accessible online through deliberate posting or sharing of information by the user.

15. Download[87] = an act of moving or copying a file, program, etc., from a usually larger computer system to another computer or device.

16. Filter[88] = Software for sorting or blocking access to certain online material.

17. Geotag[89] = A piece of data embedded in a digital media file to indicate geographical information.

18. Global Positioning System (GPS)[90] = A navigational system using satellite signals to fix the location of a radio receiver on or above the earth's surface.

19. Instant messaging[91] = A means or system for transmitting electronic messages in near real time.

20. Internet protocol address (IP-address)[92] = A number that uniquely identifies each host using the Internet.

[84] Supra note 93.
[85] Supra note 76
[86] Supra note 76
[87] Supra note 93.
[88] Supra note 93.
[89] Supra note 93.
[90] Supra note 93.
[91] Supra note 93.
[92] Supra note 93.

21. Internet service provider (ISP)[93] = An enterprise that provides services for accessing, using or participating in the Internet.

22. Online grooming[94] = The use of ICTs to undertake a process by which a person prepares a child, significant adults, and the environment for the abuse of the child. Specific goals include gaining access to the child, gaining the child's compliance and maintaining the child's secrecy to avoid disclosure.

23. Online sexual harassment and sexual exploitation- Sexual abuse and exploitation of child in online. This sexual abuse and exploitation includes "(a) The inducement or coercion of a child to engage in any unlawful or psychologically harmful sexual activity; (b) The use of children in commercial sexual exploitation; and (c) The use of children in audio or visual images of child sexual abuse; (d) Child prostitution, sexual slavery, sexual exploitation in travel and tourism, trafficking (within and between countries) and sale of children for sexual purposes and forced marriage. Many children experience sexual victimization which is not accompanied by physical force or restraint but which is nonetheless psychologically intrusive, exploitive and traumatic.[95]

"Harassment" refers to the act of "annoying or worrying somebody by putting pressure on them or saying or doing unpleasant things to them".[96]

24. Online solicitation[97] = The use of ICTs by an adult to propose to meet a child who has not reached the legal age of consent for the purpose of engaging in sexual activities or the production of child sexual abuse material.

25. Peer-to-peer (Peer2peer)(P2P) file sharing[98] = The distribution and sharing of digital documents and computer files directly between internet connected devices using a specialized software program that searches for other connected computers on a network and locates the desired resource.

[93] Supra note 93.

[94] *Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children* (2014). Commission on Crime Prevention , and Criminal Justice, United Nations Office on Drugs and Crime, p. 59, at https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_23/E-CN15-2014-CRP1_E.pdf, last visited on November 27, 2018.

[95] *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, p.12, at http://luxembourgguidelines.org/, last visited on November 27, 2018.

[96] Ibid.

[97] Ibid.

[98] Supra note 93, p. 60.

26. Sexual violence: is more and more often used as an umbrella term that includes sexual exploitation and sexual abuse.[99]

27. Sextortion: Also called "sexual extortion", is the blackmailing of a person with the help of self-generated images of that person in order to extort sexual favours, money, or other benefits from her/him under the threat of sharing the material beyond the consent of the depicted person (e.g. posting images on social media). Often, the influence and manipulation typical of groomers over longer periods of time (sometimes several months) turns into a rapid escalation of threats, intimidation, and coercion once the person has been persuaded to send the first sexual images of her/himself.[100]

28. Smartphone[101] = A device that combines a mobile phone with a hand-held computer, typically offering Internet access, data storage, e-mail capability, among other things.

29. Sexting[102] = The sending of a form of self-generated sexually explicit messages or images through mobile phones and/or the internet and typically involves minors.

30. Short Message System (SMS)/text message[103] = A short message that is sent electronically usually from one cell phone to another.

31. Social media[104] = Forms of electronic communication through which users create online communities to share information, ideas, personal messages, and other content.

32. Social networking service[105] = Online utilities that enable users to create profiles, public or private, and form a network of friends. Social networking services allow users to interact with friends via private and public means, such as messages and instant messaging, and to post user-generated content, such as photos and videos. Examples of social networking services include Facebook, Mxit, and Orkut.

[99] Supra note 85.

[100] *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, p.52, at http://luxembourgguidelines.org/, last visited on November 27, 2018.

[101] Supra note 93, p. 60.

[102] Supra note 93, p. 60.

[103] Supra note 93, p. 60.

[104] Supra note 93, p. 60.

[105] Supra note 93, p. 60.

33. Tor[106] = Tor (The Onion Router) refers to a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features.

34. Universal Resource Locator (URL)[107] = A web page's unique location or address on the Internet.

35. Web browser[108] = Software that enables users to locate, access and view web pages (e.g., Internet Explorer, Netscape, Mozilla-Firefox)

[106] Supra note 93, p. 60.
[107] Supra note 93, p. 60.
[108] Supra note 93, p. 60.

UNICEF Bangladesh
BSL Ofce Complex
1, Minto Road, Dhaka 1000
Bangladesh

Phone: +8802 5566-8088,
Fax: +8802 9335641-42
E-mail: infobangladesh@unicef.org

www.unicef.org