



KEEPING CHILDREN IN SRI LANKA SAFE AND EMPOWERED ONLINE

A study on Sri Lanka's digital landscape:
Potential risks to children and young people who are online

Commissioned by the United Nations Children's Fund (UNICEF)
Conducted by the Institute for Participatory Interaction in Development (IPID)

FOREWORD

The past decades have seen digital technology transform the world in which we live. Whilst many of us can remember life before these technologies were in mainstream use, for our children and young people who have grown up online, life is unimaginable without them.

Digital technology has disrupted entire industries and changed the social landscape. The changes they have ushered in have been broad and are ongoing. Childhood is no exception. Undoubtedly, these technologies have the potential to be a game changer for children, especially those from vulnerable and disadvantaged communities, offering them new opportunities to learn, socialize and make their voices heard. However, they can also be yet another dividing line, exacerbating and enabling inequities to prevail.

The Digital Landscape Study explores the way adolescents access and use digital technology in Sri Lanka at present. While identifying gaps in knowledge about children's digital media practices and their online safety, the report provides some key recommendations for government, NGO's and the private sector that will help to ensure that digital technologies, and the access to the internet that they afford, bring the maximum benefits to children and young people individually, and to their communities and the country as a whole.

Key to this will be a more proactive approach to protecting children from harm - including abuse, exploitation, trafficking, cyberbullying and exposure to unsuitable materials - and securing their privacy as they become prone to risks both online and off line. Also vital will be ensuring equal access to these technologies and the internet to all children and young people, irrespective of gender or geographical location. Of further importance will be ensuring our young people are digitally literate, and able to make the best, and most informed use of the digital tools at their disposal.

This report gives us all, as citizens living in an increasingly digitalized and online society, and as parents, guardians, teachers, and members of the government, private sector and NGOs, the knowledge and insight needed to ensure we maximise the real opportunities provided by digital technology to children, whilst minimizing the risk of harm.



Tim Sutton
Representative, UNICEF Sri Lanka

MESSAGES

Message from the Secretary, Ministry of Education

It is a privilege to provide a message for the study report on socio-cultural factors influencing children's online behaviour conducted by UNICEF.

The ministry of education facilitated the study allowing access to study population consisting of school children, principals, ICT teachers and trainers.

The Internet opens a door to the world's largest resource repository. However, the threats associated with the Internet cannot be underestimated. Therefore, the study on children's use of the internet, their digital media practices and online safety is a timely concern. Further it is my belief that the recommendations provided by the survey will definitely help to improve the awareness programmes and align policy framework on effective use of the Internet and online safety.

I would like to express my gratitude towards UNICEF for taking up the challenge of this timely requirement and wish them good luck in their future endeavours.

Sunil Hettiarachchi

Message from the Secretary, Ministry of Telecommunication and Digital Infrastructure

Commissioning a study to understand the 'digital landscape' in Sri Lanka and the potential risks to children and young people by UNICEF in 2015 is a commendable effort. The findings of this study will provide information which would help to strengthen policy in this important area. Further it will lead to a safer online environment for children and young people in Sri Lanka.

Security and safety of children online has become a major concern to the government and other international organizations. Protecting children who are online is a global priority. Ensuring the online safety of children is crucial, the issue of safety of children has to be addressed in the context of their digital rights. Children use the Internet to express their pent-up desires and are thereby exposed to many risks and become vulnerable to online predators. The current global trend in development is based on rights. In this context, children have a right to health, education, information, voicing their opinions and to engage in society as civilians. Many of these rights are achieved, to some degree, through a child's access to digital technology. Therefore institutional duty bearers of online children have to strike a balance between online risks and benefits.

Over the last decade, Sri Lanka has recognized IT as a priority area for government intervention. Education and ICT policies, of the government have contributed to expanding awareness, accessibility and affordability of ICT. The telecentres, established by the government in rural areas under the Nenasala programme of the eSriLanka initiative, the IT labs established under Mahindodaya programme, the e-learning programmes such as SchoolNet and the e-Thaksalawa programmes have contributed to improving ICT awareness and access among children in Sri Lanka.

Realizing the complexity of these issues, UNICEF supported studies in several instances to examine the ground realities to help the relevant stakeholders take appropriate actions to mitigate the threats and enhance the benefits.

I commend the UNICEF and all involved in this laudable exercise.

Wasantha Deshapriya

ACKNOWLEDGEMENTS

Executive Director, Institute for Participatory Interaction in Development (IPID)

We owe our gratitude to Ms. Una McCauley, former Sri Lanka Country Representative, UNICEF; Ms. Misbah Sheikh, former Chief of Communication, UNICEF, Sri Lanka; and Ms. Suzanne Wooster Prematilaka, Communications Officer, External Relations, UNICEF, Sri Lanka, for the invaluable cooperation extended by them to the Institute for Participatory Interaction in Development (IPID) and to the consultancy team for the successful completion of this study.

The guidance and suggestions provided by the steering committee, and the ethical clearance granted by the ethical review committee, Faculty of Medicine, University of Peradeniya, contributed immensely in facilitating the implementation of the study which involved different stakeholders.

We offer our gratitude to Mr. Neil Gunadasa, Director-IT, Ministry of Education, for his invaluable contribution and to the various officers at the national, provincial and zonal levels of the ministry for providing necessary approvals and support to conduct the study in the school system.

We offer our thanks to the principals of the selected schools for facilitating the administration of the questionnaire. IPID also acknowledges the cooperation extended by the teachers, students and parents who participated in the study. We wish to acknowledge the information shared and the courtesies extended by the stakeholders, to the visiting teams, during the Key Informant Interviews (KIIs).

IPID extends its sincere thanks to the team for its dedication and hard work, without which it would not have been possible to successfully complete this study. In this context, IPID wishes to acknowledge and appreciate the professional contributions made by Prof. Karunatissa Atukorala as the principal researcher and by Dr. Harsha Liyanage as the ICT and digital landscape expert, which added great value to the study.

Finally, we wish to express our appreciation of the opportunity provided by UNICEF Sri Lanka to IPID, in assigning the study on 'Keeping Children in Sri Lanka Safe and Empowered Online'.

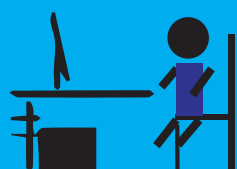
S. W. K. J. Samaranayake

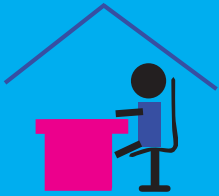
ACRONYMS & ABBREVIATIONS



CONTENTS

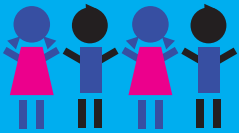
Foreword	i
Message from the Secretary, Ministry of Education	ii
Message from the Secretary, Ministry of Telecommunications and Digital Infrastructure	iii
Acknowledgments	iv
Acronyms & Abbreviations	v
The Study Team	x
Technical Steering Committee	x
Executive Summary	xi
1. INTRODUCTION	1
1.1 Background	1
1.2 Objectives	2
1.3 Methodology	2
1.3.1 Study design	2
1.3.2 Data collection	2
1.3.3 Preparation for data collection	3
1.3.4 Limitations and challenges	4
2. CHILDREN AND THE DIGITAL LANDSCAPE IN SRI LANKA	5
2.1 Online access and children's rights	5
2.2 ICT awareness	6
2.3 Institutions responsible for the online safety of children	9
2.4 The digital divide	9
3. CHILDREN WHO ARE NOT ONLINE IN SRI LANKA	11
3.1 Introduction and definitions	11
3.2 Distribution of respondents	12
3.3 Status of non IT users	15
3.4 Status of non-online IT users	16
3.5 Reasons for not accessing the internet	17
4. ONLINE BEHAVIOUR OF CHILDREN IN SRI LANKA	20
4.1 Introduction	20
4.2 Age of first access	20
4.3 Devices used for access	21
4.4 Source of computers used for access	22
4.5 Internet access through dedicated institutions	23
4.6 Sources of income for access	26
4.7 Frequency of access	27
4.8 Learning how to access the internet	29
4.9 Reasons for accessing the internet	29
4.10 Frequently accessed websites, apps and social media	32
4.11 Children's online interactions	40
4.12 Positive online experiences	42
4.13 IT teachers in government schools	44
4.14 The knowledge gap between online-IT users and duty bearers/key stakeholders	45





5.	ONLINE SAFETY OF CHILDREN IN SRI LANKA	47
5.1	Introduction	47
5.2	Threats: The global perspective	48
5.3	Risk vs harm: The global perspective	49
5.4	Risks to online-IT users	49
5.5	Indicators of exposure to risk	52
5.6	Reporting process for online abuse	56
5.7	Learning about online safety	57
5.8	Policy issues on online safety	58
5.9	The role of institutions and their capacity	59
5.10	Appropriate age of access	60
5.11	Parental control of internet use	60

6.	RECOMMENDATIONS	61
-----------	------------------------------	-----------



LIST OF TABLES

Table 1	Number of children in the sample: by category	2
Table 2	Computer literacy rate by Gender, Age, Level of Education and Language Literacy, 2014 6-7	
Table 3	Number of children in the different IT user levels, in the government-schools category: by sector, ethnicity and gender.....	12
Table 4	Reasons for not using a computer or a mobile phone, as expressed by non-IT users.....	15
Table 5	Source of computers and mobile phones used by non-online-IT users.....	16
Table 6	Amount spent per month on mobile phone usage by non-online-IT users.....	17
Table 7	Source of funds for children's monthly mobile phone bill.....	17
Table 8	Reasons for not accessing the Internet, as expressed by the non-online-IT users.....	18
Table 9	Desire to access the Internet as expressed by the non-online-IT users.....	19
Table 10	Average age of first access of the Internet: by gender, sector and ethnicity.....	20
Table 11	Technology related job preferences by gender.....	21
Table 12	Type of digital device used by children to access the Internet: by gender.....	21
Table 13	Type of digital device used by children in government schools to access the Internet: by ethnicity and sector.....	22
Table 14	Source of computers used by online-IT users to access the Internet.....	23
Table 15	Number of online-IT users that accessed the Internet from dedicated institutions.....	23
Table 16	Data on the student population, computer availability and internet access (Grade 6 and above) in government schools.....	24
Table 17	Monthly expenditure on mobile phone and Internet usage by online-IT users.....	26
Table 18	Source of funds to pay for mobile phone and Internet bills.....	26
Table 19	Frequency of children accessing the Internet: by gender, sector, ethnicity, grade & province.....	27-28
Table 20	Mode of learning to access and use the Internet: by gender and ethnicity.....	29
Table 21	Reasons why children access the Internet by gender, ethnicity and sector.....	30-31
Table 22	Top 20 most popular websites and apps of the Sri Lankan public.....	32
Table 23	Websites and apps accessed by children: by gender and ethnicity.....	36
Table 23.1	Websites and apps accessed by children: by grade.....	37
Table 24	Frequently accessed sites/apps by adolescents, especially in grades 10-12 ¹⁰	39
Table 25	Reasons for using Facebook, as expressed by children with Internet access by gender & ethnicity.....	40
Table 26	Persons with whom children communicate using social media: by gender, ethnicity and sector.....	42
Table 27	The most memorable, positive experiences of online-IT users, percentage.....	44
Table 28	Children's response (as percentage of sampled population) to online strangers' requests for personal information: by gender, ethnicity and grade.....	50
Table 29	Response to the query on physically meeting people, previously met online, as a percentage of sampled population, by gender.....	50
Table 30	Action taken during offline meetings with strangers befriended online, percentage of sampled population by gender.....	51
Table 31	Action taken by children online to change the privacy settings of their online accounts: by gender, grade, sector and ethnic origin.....	51-52
Table 32	Indicators of exposure to risk: as a percentage of sampled population by gender.....	53
Table 33	Percentage of children who shared inappropriate content online.....	54
Table 34	Children's knowledge on where to report online abuse.....	56
Table 35	Children's sources for learning how to protect personal information and privacy online as a percentage of sampled population.....	57
Table 36	Children's preferred sources for learning about protecting personal information and privacy online: as a percentage of sampled population.....	57

LIST OF FIGURES

Figure 1	Computer literate persons, aged 5-69, as a percentage of the population in 2006/07, 2009 and 2014: by province	7
Figure 2	Household computer ownership in Sri Lanka from 2004 to 2014	8
Figure 3	Mobile telephone subscriptions and Internet users, as a percentage of the population in Sri Lanka from 2005 to 2013	8
Figure 4	Distribution of children (11-18 years of age): by IT-user levels	12
Figure 5	Composition of IT users (as a percentage): by gender	13
Figure 6	Composition of IT users (as a percentage): by sector	13
Figure 7	Composition of IT users (as a percentage): by ethnicity	14
Figure 8	Composition of IT users (as a percentage): by school grades	14
Figure 9	Composition of IT users (as a percentage): by province	15
Figure 10	Percentage of children using social media and apps: by gender, ethnicity and sector ...	34
Figure 10.1	Percentage of children using social media and apps: by school, grade and province ...	35
Figure 11	Percentage of access to social media and apps: by gender	38
Figure 12	Percentage of access to social media and apps: by grade	38
Figure 13	Percentage of access to social media and apps: by ethnicity	38
Figure 14	Individuals that children communicated with online: by gender	41
Figure 15	Children engaged in risky behavior: as a percentage of sampled population	55

THE STUDY TEAM

1. Prof. S. Karunatissa Atukorala, Principal Researcher
2. Dr. Harsha Liyanage, ICT and Digital Landscape Expert
3. Ms. Mallika R. Samaranayake, Education and Child Protection Expert
4. Ms. Praneetha Abeywickrema, Legal Expert in Child Rights and Communication
5. Mr. Amil Jeewan Kithsiri Epa, Project Manager
6. Ms. Hasara Kalubowila, Researcher
7. Ms. Nina Abeydeera, Researcher and Coordinator (Private and International Schools)
8. Mr. N. M. Mohideen, Translator and Coordinator (Tamil Medium Schools)
9. Mr. Anura Fernando, Translator and Coordinator (Sinhala Medium Schools)
10. Mr. Thishan Lakmal, Team Member
11. Mr. Jagath Kumara, Team Member
12. Ms. Manjula Dissanayake, Team Member

TECHNICAL STEERING COMMITTEE

The study was informed and guided by a Technical Steering Committee. In this respect UNICEF and the Institute for Participatory Interaction in Development acknowledge the valuable technical inputs of the following steering committee members:

Mr. G.M. Neil Gunadasa

Director, Information and Communication Technology, Ministry of Education

Mr. Roshan Chandraguptha

Information Security Engineer, Sri Lanka Computer Emergency Response Team

Mr. Sanjana Hattotuwa

Special Advisor, Senior Researcher, Centre for Policy Alternatives (CPA) and ICT4 Peace Foundation

Ms. Shalini Ratwatte

Head of Legal & Corporate Affairs, Microsoft Sri Lanka (Pvt) Ltd.

Mr. Gopiharan Perinpam

Technical and Digital Media Expert

EXECUTIVE SUMMARY

The Internet has created enormous opportunities for children's development, but also exposes them to an evolving set of risks. Parents and guardians have a duty to balance the risks and benefits of online access so that young people can realize their rights under the Convention on the Rights of the Child, including their right to access to information (Article 17).

Realizing the complexity of these issues, UNICEF supported studies in several countries to examine the on-the-ground realities and to help the relevant stakeholders develop appropriate responses. Prior to this, no national level study had been conducted to analyze the online behaviour of children in Sri Lanka. This study mapped the landscape of children's access and usage of the Internet in Sri Lanka, identified gaps in knowledge about children's digital media practices and their online safety, and recommends opportunities to improve children's online safety at the government, NGO and private sector levels.

Using qualitative and quantitative methodologies, the study focused on children 11-18 years old through a survey of 5,349 children in 73 government, private schools and telecentres. Researchers also collected additional data from school principals, IT teachers, parents, children who were 'heavy' IT users, and key policy makers.

The digital landscape in Sri Lanka is evolving. Recognizing the need for IT education across the country, the government has established over 600 rural telecentres, ICT labs and various e-learning programmes. In 2014, one in four Sri Lankans was computer literate. As of 2013, countrywide mobile telephone coverage was 95 per cent, and 57 per cent of the Internet users used mobile telephones to access the Internet.

However, despite many positive developments, inequality of online access and usage is still a major issue in Sri Lanka. Mobile broadband coverage in isolated rural areas is slow, Internet connections at school labs are slow or non-existent, and school administrators heavily control access to the Internet in most public schools. Inadequate translations of government and commercial websites into the vernacular have contributed to limited access by the public, and at times, by children.

Types of IT Users

The study categorized groups of IT users based on the following:

- **Non-IT users:** Seven per cent of children surveyed had no access to any digital device, with parental control being the top deciding factor. Nearly 56 per cent of this group were not allowed to use a mobile telephone and 20 per cent were not allowed to use a computer. Parents' inability to afford either a computer (49.3 per cent) or a mobile telephone (31.5 per cent) was another major reason. Interestingly, a significant proportion of the non-IT users reported that they personally disliked using computers (29 per cent) or mobile telephones (42.5 per cent).
- **Non-online IT users:** Around 40 per cent of children surveyed had access to a computer or digital device, but were not able to access the Internet. Around 89.4 per cent of children in this group had access to mobile phones and 48.3 per cent to computers, but were restricted by lack of Internet access on their digital devices or discouragement by parents and teachers. However, 24.7 per cent of the students in grades 6-9, 28.4 per cent in the Ordinary Level classes and 35.5 per cent in the Advanced Level classes reported that it was their personal choice not to access the Internet.
- **Online-IT users:** About 53 per cent of respondents of the urban sector were online users followed by, 47.1 per cent in the rural sector and 37.3 per cent in the plantation sector. The majority (67.6 per cent) of these users were boys. Two-thirds (67.8 per cent) of urban dwellers surveyed were online users, about half of respondents in the rural sector were online users (47.1 per cent) and only 39.3 per cent of plantation sector were online IT users. On average children in the online-IT user group started online activity at the age of 13 years, although some started as early as five years. Children used mobile phones and computers (some used both devices) to access the Internet. In government schools, 74.8 per cent of this group of children used mobile phones and 66.5 per cent used computers to access the Internet. On the other hand, in private schools, 80.9 per cent students accessed the Internet using computers. On average, about one-third of the online-IT users used their own computers to access the Internet.

Children's Usage Patterns

Over half of the online-IT users (53.6 per cent) learned to access the Internet by themselves, and a higher proportion of boys (60.3 per cent) than girls (35.1 per cent) were self-taught. Nearly half of the girls (47.3 per cent) learned to access the Internet from their siblings.

Children said they accessed the Internet to search for information for educational purposes; download information or videos; watch online content; access social media; listen to the radio; and play online games. Facebook was the most popular social platform and was far more popular with boys (72 per cent) than girls (33 per cent). Skype, Viber and WhatsApp were other top digital platforms accessed by children. Children said that they used social media to chat with friends and communicate with relatives in distant places. Children received a range of benefits by being online. More than half of online users said that they obtained their examination results online.

This study also found that the facilities available at *Nenasala* and computer training institutes were rarely used by children to access the Internet. The schools played a very limited role as only 11 per cent of the children used school computers for online activity.

Types of threats experienced by children

This study identified several online threats to children. Both boys and girls at times communicated with people that they had only met online and never in person, a finding with major implications for online safety. More boys than girls reported arranging in-person meetings with people they had met online.

Some children in the online-IT user group faced online identity threats, such as requests to make payments to obtain the lottery prizes they were said to have won, and invitations to meet online friends they had not physically met before. Nearly 25 per cent of the online-IT users were not aware of the privacy settings for their online accounts and therefore were exposed to potential online threats. About 10 per cent of the children admitted to uploading or sending online material inappropriate for their age and 41 per cent admitted to sharing photographs and personal information online with unknown people. There was some indirect evidence to suggest that children, knowingly or otherwise, infringed on copyright laws, and engaged in online identity theft and cyber bullying.

As children accessed the Internet primarily at home or school, their parents and teachers were their key duty bearers. IT teachers appeared to be inactive in taking positive actions to reduce online risks and threats. The study revealed that the majority of parents were not aware of the extent of online access, online risks and what their children were up to at home or school.



Recommendations

Based on these findings, this study has formulated a set of recommendations which have been drawn up using international guidelines and the opinions of a diverse set of national experts. The core strategic objective of the recommendations is to protect children who are online, based on the principles of empowerment rather than control.

The recommendations of this study focus on:

- Policies, laws and regulations to strengthen a national policy framework on the online security of children, including a review of current regulations, creating new regulations and modifying existing laws.
- Advocacy and capacity building to develop campaigns on safe Internet usage and strengthen national understanding of patterns of digital usage amongst children. It is also important to improve the capacities of law enforcement and regulatory organizations on child protection in the online sphere.
- Introduction of specialized technology to enable safe online usage for young children, and the promotion of parental controls and age verification processes.
- Encouraging school and community-based children's societies to work towards creating awareness and enabling children to benefit from the Internet in a safe and protected environment.
- Review of school curricula for safe Internet use and more active promotion of the e-thaksalawa materials from the Ministry of Education.

This study, commissioned by UNICEF, has contributed significantly towards understanding the key characteristics of the digital landscape in the lives of children in Sri Lanka. Its main focus is on protecting children from online threats while empowering them on the safe use of the Internet and responsible digital citizenship.

1. INTRODUCTION

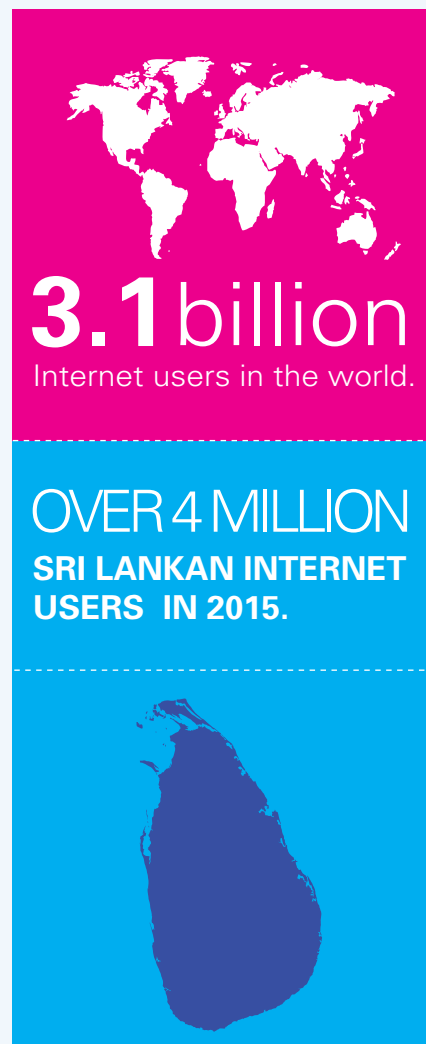
1.1 Background

There are over 3.1 billion Internet users in the world. Almost half of them are in Asia and Sri Lanka recorded over 4 million Internet users in 2015 (Internet Live Stats). The Internet is a dynamic resource, and children¹ access the Internet to learn, communicate, play, participate, innovate and socialize through digital devices including computers, laptops, mobile phones, smart phones, tablets and game console stations. While the Internet provides new opportunities it also exposes children to evolving risks. Therefore, protecting children who are online is a global priority.

Children use the Internet to explore, express and satisfy their curiosity, which may expose them to risks including online predators. All over the world, children¹ have a right to health, education, to access information, to voice their opinions and to engage in society as citizens. Many of these rights are achieved, to some degree, through a child's access to digital technology. Institutional duty bearers have to strike a balance between online risks and benefits to children's access and usage of online materials. This complex issue needs to be carefully monitored with child-appropriate interventions when necessary. Ensuring the online safety of children is important, but it needs to be understood in the context of the spectrum of their digital rights.

The UN Convention on the Rights of the Child² sets out the rights that must be realized for children to develop to their full potential, and to be free from hunger, neglect and abuse. Reviews of the Convention have shown significant progress in some areas of children's rights, including declining infant mortality, rising school enrollment and better opportunities for girls. However, despite overall gains, the safety and security of children who are online is a new and challenging area in ensuring that all children are able to realize their rights (UNICEF, 2014).

Post-conflict Sri Lanka has made significant progress in introducing information and communications technology (ICT) into its national development agenda. The Government of Sri Lanka (GoSL) has recognized information technology as a priority area, contributing to the improved awareness, accessibility and affordability of ICT (Department of National Planning, 2010). In this context, the online security and safety of children demands the serious attention of policy makers.



¹ The United Nations Convention on the Rights of the Child defines child a person under the age of 18.

² The Convention on the Rights of the Child is the United Nations treaty of 1990 that specifies the rights of children. It has been ratified by almost all the UN-member states, including Sri Lanka.

1.2 Objectives

This study aims to contribute towards developing strategic interventions for UNICEF Sri Lanka and its partners to address issues of children's online safety. It has three objectives:

1. Map the key characteristics of the digital landscape³ in Sri Lanka as it relates to children's access and use.
2. Identify knowledge gaps and constraints in children's digital media practices and online safety.
3. Recommend opportunities to leverage and strengthen existing government, non-governmental organization, private sector and global initiatives, to promote safe and engaged digital citizenship to benefit all children, including marginalized children.

1.3 Methodology

1.3.1 Study design

The study adopted a mixed methodology to collect both qualitative and quantitative data. The target groups of the study were children, defined as individuals under the age of 18. To supplement the data, parents, teachers, principals and other national level stakeholders were included in the study. In mapping the online behaviour of children in Sri Lanka, a survey was used to collect quantitative data and a descriptive method was used to collect qualitative information on socio-cultural factors relating to online behaviour.

1.3.2 Data collection

Five major data collection instruments were used in the study.

Secondary data: The study reviewed research documents, national policy documents, international conventions, mass media output and project reports relating to online accessibility, child rights and safety issues. The purpose was to map the stakeholders, list the broader issues and assess the gaps in knowledge in the current national context as against international best practices. This helped to understand the macro view of online behaviour and to determine the data collection tools this study needed to focus on.

Sample survey of children: The study conducted a survey of 5,349 children aged 11-18 years in Grades 6 to 12 in schools, using a stratified random sample to select the schools. The school population was categorised according to the type of school (government and private, including international) and the sample was selected to represent these school types. The sector (urban, rural and plantation), was determined by the location of the school. A questionnaire-based survey covered 65 government schools, eight private schools, including international schools, and 10 telecentres⁴ (e.g. Nenasala and Information Technology Training Centres). The sample also balanced gender, age and ethnicity.

Table 1: Number of children in the sample: by category

Category	Number of children
Government schools (urban, rural & plantation)	4,845
Private schools, including International schools	429
Telecentres	75
Total	5,349

³ The digital landscape is defined in this study as the parameters of children's access to the Internet. The ranges include the use of different digital devices to engage with varying types of content, including social networks, websites, email and other communications tools, apps, videos and games.

⁴ Telecentres are service providers who provide Internet access, they also conduct basic level IT classes and provide international calling, typesetting, photocopying/bookbinding, faxing and other related services. Customers include both children and adults.

Three different surveys were administered to children depending on which of the following categories they fell into: 1. Non-IT users (children with no access to a digital device or the Internet); 2. Non-online IT users (children who had access to a digital device but not to the Internet); 3. Online IT users (children with access to a digital device and access to the internet). The questionnaires were child-friendly, participatory and self-administered, with each user group guided by 2-3 facilitators.

The researchers also collected school data from 60 principals through a checklist, including the total student population, availability of an IT lab, availability of computers, availability of an Internet connection and the school's information communication technology (ICT) policy.

Focus group discussions: Building on the questionnaires, researchers conducted focus group discussions to collect qualitative information from students who were heavy online-IT users who accessed the Internet, including social media, several times per week. Researchers held 66 focus group discussions with 696 children representing government and private schools. Researchers also conducted 29 focus group discussions with 216 parents to understand their own perceptions of their children's digital usage.

Key informant interviews: Researchers conducted 17 key informant interviews with government policy makers (including the Ministry of Education and the National Child Protection Authority), and with international organisations such as UNICEF, national opinion leaders, media personnel (print and electronic), academics, NGO leaders and corporate leaders in the telecommunications and software industries. The key informant interviews outlined policy issues related to the online security of children, services provided, and readiness and limitations faced by the authorities responsible for these issues.

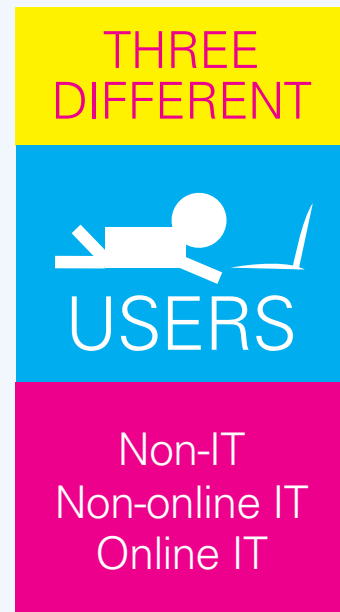
There were also 77 key informant interviews conducted with school teachers to find out their views on the online habits and safety of students.

Case studies: Based on data from secondary sources, media reports and the field experiences of the consultants, three case studies were developed. These case studies were designed to focus on how children were exposed to risks and rewards from online exposure within their sociocultural settings. These case studies helped to ascertain different aspects of risks and rewards.

1.3.3 Preparation for data collection

Training the study team: All facilitators, investigators and data entry operators were trained before data collection began through a four-day training course. The first two days covered the conceptual aspects and the data collection tools of the study, and the third and fourth days covered field work. The training covered data collection techniques, data collection tools, rapport building, facilitation methods and research ethics.

Pre-testing: The data collection tools were pre-tested at a school in Colombo in all three language streams (Sinhala, Tamil and English) and with all three major ethnic groups (Sinhalese, Tamil and Muslim), as well as at a Telecentre in a rural area. Based on the responses, the data collection tools were improved and tested again at three schools in Colombo to check the appropriateness of the questionnaires to the target group and the context. The questionnaires were modified again after this test.



1.3.4 Limitations and challenges

The study faced a number of limitations and challenges.

First, there were delays in obtaining ethical clearance, leading to the school survey taking place in the third term rather than the first term of 2015. School authorities were rather hesitant to give permission due to impending examinations and the need to complete the syllabi on time.

Second, many of the originally selected private schools declined to respond to the study. Therefore, an additional sample of private schools, including international schools, was selected to achieve the target. In some private schools, a significant number of parents did not allow their children to participate in the study, and those schools were replaced by the sample buffer.

Third, attendance of parents to focus group discussions was low. In government schools, 28 out of 30 focus group discussions were completed and only one out of five was completed in private schools.

2. CHILDREN AND THE DIGITAL LANDSCAPE IN SRI LANKA

2.1 Online access and children's rights



Sri Lanka is among the 67 United Nations member states that ratified the Convention on the Rights of the Child (CRC) in 1991 within one year of its adoption. Among the 54 articles of the CRC, the following merit the attention of this study: Article 12 – respect for the views of the child; Article 13 – freedom of expression; Article 16 – right to privacy; Article 17 – access to information; and Article 19 – protection from all forms of violence.

67

UNITED NATIONS
MEMBER STATES
RATIFIED CRC

After ratifying the CRC, Sri Lanka's cabinet approved a newly-formulated national children's charter, based on the CRC, into state policy (Wijemanne, 2014). The National Child Protection Authority (NCPA) was established in 1998 as an outcome of recommendations by the presidential task force for child protection. With the mission to "...ensure children are free from all forms of abuse," the NCPA currently operates under the purview of the Ministry of Child Development and Women's Affairs (NCPA, 2016). The state's concern to protect children from child abuse through Internet 'grooming' was noted in Sri Lanka as early as 2002.

Sri Lanka has made significant and consistent progress in many aspects of the CRC, including the right to health and education. Efforts have also been taken to adopt information and communications technology (ICT) into the national development agenda. In this context, online security and safety of children is receiving the serious attention of policy makers. For instance, in 2015, the NCPA appointed a task force to combat the online security threats faced by children (Karunarathne, 2015).

Over the last decade, around the world, the implementation of the CRC has been met with new challenges due to the complexities the Internet has introduced into children's social interactions. The Internet and digital devices have provided the means for children to participate in the global society in ways previously not possible. For example, being online enables children to broaden their education, gain access to important information, evolve as citizens, mobilize on issues that concern them, gain awareness about other cultures and become informed, global citizens. The Internet also exposes children to violence, inappropriate content and raises concerns about excessive use. In this context, it is essential to understand how this changing environment impacts the wellbeing of children and their rights.

Third et al (2014) argue that ensuring the online safety of children is vital, but needs to be understood in the context of the spectrum of their digital rights. According to the same study, regardless of the country, language or socio-economic background, if children have access to the Internet, they tend to use it for a common set of purposes: social connectedness, access to information, education, self-expression and creativity, and entertainment. Children also recognize the Internet as crucial to their rights to information, education and participation. Therefore, in terms of online child protection, it is important to find ways to foster children's right to protection from harm, while simultaneously empowering them to maximize the benefits of being online.

2.2 ICT awareness

Over the last decade, Sri Lanka has recognized IT as a priority area for government support. The government's education and ICT policies (Department of National Planning, 2010) have contributed to expanding awareness, accessibility and affordability of ICT. Over 600 Telecentres were established by the government in rural areas under the Nenasala programme, part of the eSriLanka initiative. At the same time, the IT labs installed under Mahindodaya programme, the e-learning programs such as SchoolNet and the e-Thaksalawa programmes have contributed to improving ICT awareness and access among children in Sri Lanka.

In this context, the online community of children is growing rapidly. One in four people in Sri Lanka was computer literate⁵ in 2014; computer literacy has risen from 16 per cent to 25 per cent over the last eight years (Department of Census and Statistics, 2014). Children and youth have the highest computer literacy rates. Such improvements in computer literacy were observed in all provinces, including the Northern and Eastern Provinces, even though they were affected by the ethnic conflict until 2009 (Figure 1).

Table 2: Computer literacy rate by Gender, Age, Level of Education and Language Literacy, 2014

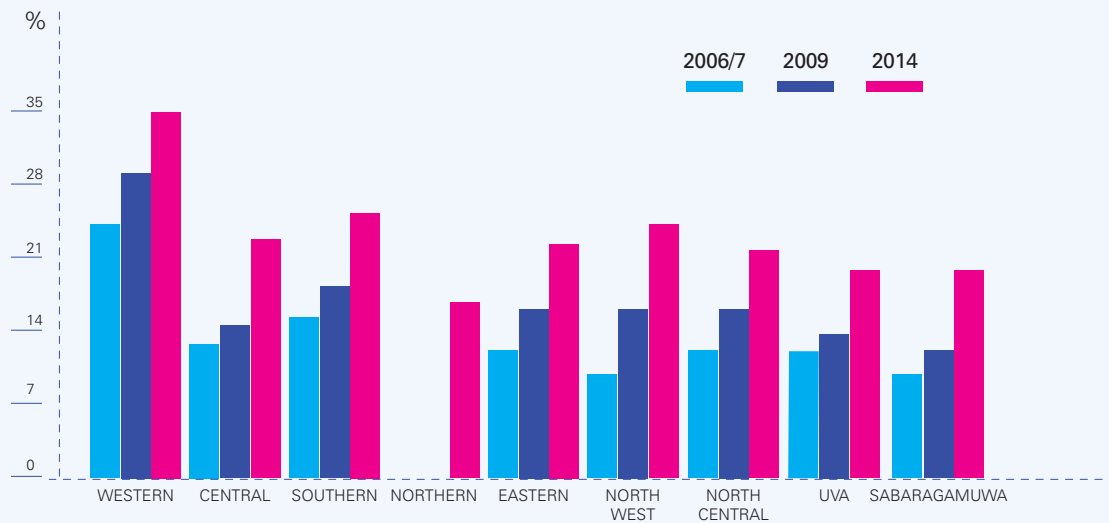
	Computer literacy rate (%)
Sri Lanka	25.1
By Gender	
Male	27.0
Female	23.3
By Age group (years)	
5 - 9	12.3
10 - 14	36.5
15 - 19	54.4
20 - 24	49.3
25 - 29	40.3
30 - 34	30.3
35 - 39	23.5
40 - 49	15.4
50 - 59	9.3
60 - 69	6.0

⁵ **Computer literacy:** A person (aged 5-69) is considered as a computer literate person if he/she can use a computer on his/her own. For example, even if a 5 year old child can play a computer game then he/she is considered as a computer literate person. **Computer literacy rate:** Computer literate population expressed as a percentage of the total population (aged 5-69 years), within the respective domain.

Table 2: Contd.

Computer literacy rate (%)	
By Educational attainment	
No schooling.....	0.5
Below grade 6.....	8.9
Grade 6 - 10.....	16.1
G.C.E. (O/L).....	39.0
G.C.E. (A/L) or above.....	68.0
By Language literacy	
Sinhala.....	30.4
Tamil.....	25.1
English.....	67.3

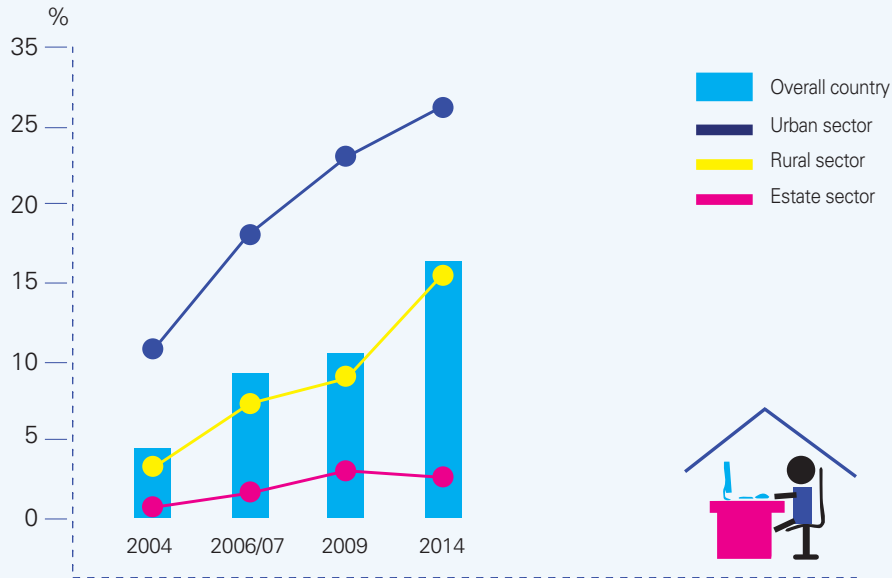
Figure 1: Computer literate persons, aged 5-69 years, as a percentage of the population in 2006/07, 2009 and 2014: by province



Source: Computer literacy statistics, 2014, the department of census and statistics of Sri Lanka.

The overall increase in household computer ownership (up to 16.6 per cent in 2014), combined with improved computer education through schools, private providers and civil society institutions, have contributed to an increase in the computer literacy rate.

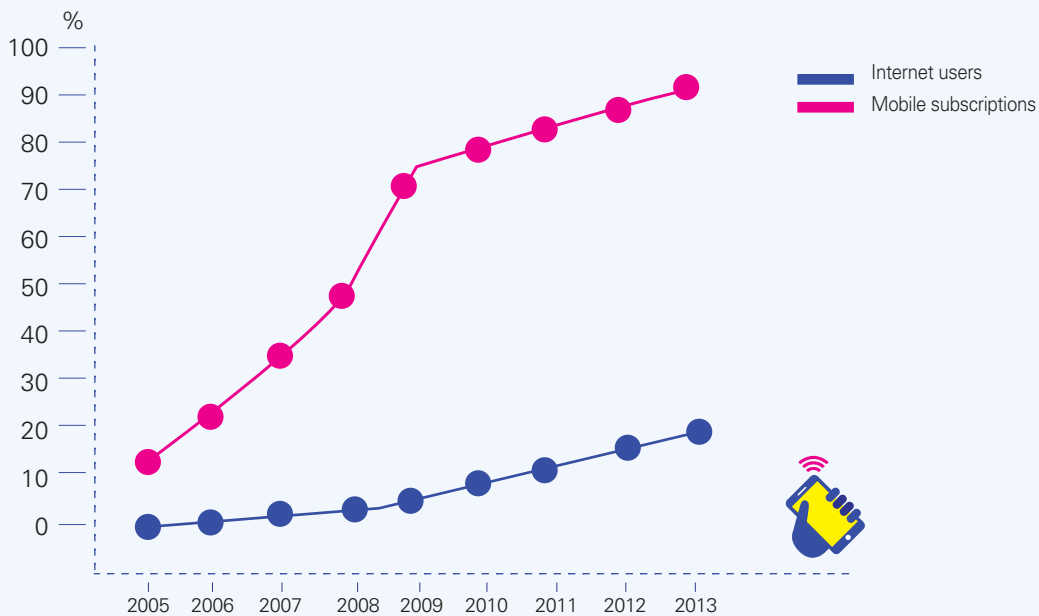
Figure 2: Household computer ownership in Sri Lanka - 2004 to 2014



Source: Sri Lanka, Department of Census and Statistics (2004, 2006/07, 2009, 2014)

As of 2013, countrywide mobile coverage and affordability enabled 95 out of every 100 people to have access to mobile phones, opening up opportunities to access a range of voice and data services. Of the 2.8 million Internet users in Sri Lanka at the end of 2013 (Nielsen Consumer Surveys, 2014), 24 per cent of users aged 15 to 60 accessed the Internet and out of them 57 per cent through their mobile phones. In the general population, 47 per cent of Internet users were between 15 and 25 years old and about 21 per cent accessed the Internet at least once per week.

Figure 3: Mobile phone subscriptions and Internet users as a percentage of the population in Sri Lanka (2005 to 2013)



Source: World Data Bank (2014)

2.3 Institutions responsible for the online safety of children

National Child Protection Authority (NCPA) of Sri Lanka was established by the parliament in 1998, and it is a leading authority for the protection of children from all forms of abuse. The NCPA operates under the purview of the Ministry of Child Development and Women's Affairs. It advises the government, consults relevant line agencies, including law enforcement authorities, coordinates an island-wide network of field officers to create awareness, implements projects, monitors investigations and recommends legal reforms.

Sri Lanka Computer Emergency Readiness Team (SL-CERT) of the National Centre for Cyber Security is a key focal point for cyber security in Sri Lanka. As a subsidiary organization of the government's Information and Communication Technology Agency (ICTA), SL-CERT provides expertise, technical support and security alerts.

UNICEF Sri Lanka, through its child protection portfolio, promotes children's online safety through campaigning, awareness raising and research. In 2014, it used the occasion of the 25th anniversary of the CRC to launch a series of high-level policy discussions that led to a public reaffirmation of a commitment to child rights by key stakeholders such as ministers, parliamentarians and the national media. UNICEF Sri Lanka has partnered with the Centre for Peace Building to increase the capacity of children for reporting through video and photography, and to encourage adolescents to share their stories through social media.

Sarvodaya-Fusion is the ICT for development arm of Sarvodaya, one of the leading national NGOs. The organization promotes IT education among rural communities across Sri Lanka. In collaboration with 75 rural Telecentres, the majority of which were installed by the Information and Communication Technology Agency under the eSriLanka programme in 2006, Sarvodaya-Fusion educates over 1,500 children and youth annually on basic IT, social media and android technologies. 'IT Yaha-Maga' (the right way of using IT) is their latest campaign to educate rural youth and adults on the appropriate use of social media.

Other institutions engaged in work related to online security of children in Sri Lanka include the Ministry of Education, the Ministry of Justice, ICTA, the Department of Police and Microsoft. Most of these institutions work in collaboration on online security issues. For instance, the NCPA is working with these institutions and several private sector organizations, NGOs and INGOs to develop a module for school children (NCPA, 2015) on the safe use of the Internet with a special focus on cyber bullying and other cyber-crimes.

2.4 The digital divide

There is almost island-wide mobile signal coverage and affordable mobile data services including in rural areas. Key informants in this study highlighted the accessibility of these services as an equalizer, compared to other conventional technologies.

There is also increasing availability of local language content (in Sinhala and Tamil) compared to five years ago when it was a major barrier. Google Translate and Facebook are also available in both local languages. Facebook has become a common meeting ground with comments made in Sinhala and Tamil.

However, key informants note that inequality exists in terms of 'quality' and 'accessibility' all over Sri Lanka.

First, given the rapid pace of the advancement of technology (for example from mobile phones to smart phones and 3G to 4G mobile technologies), the penetration of these technologies to the deep rural pockets remains rather slow⁶. Some rural communities do not have access to 3G mobile coverage, and smart phones are unaffordable to many.

Second, key informants note that language remains a barrier, as most public services such as banking are not sufficiently tri-lingual leading to lack of access. For instance, some government websites do not have facilities for Tamil language translations of their content.

Third, the focus group discussions highlighted that Internet speed in most rural schools remains very slow, and computers and Internet connections in school computer labs are not updated. The combined effects of these factors limit access and quality of Internet services for students from the rural and plantation sectors.

⁶ Observations shared by Sarvodaya-Fusion as per their direct project experiences; SMART Villages and Android Hubs, implemented in rural pockets together with Etisalat Ltd. 2014

Fourth, low income families from the plantation sector and urban households cannot afford computers and broadband access. Therefore, public schools remain the key point of access for their children. The computer to student ratio is adversely low in a majority of schools, discouraging many students from using the school computer lab to access the Internet. In addition to the low numbers of computers in schools, most students below Grade 6 are not allowed access to school computer labs and access to computers is controlled by school authorities such as principals and IT teachers. These factors contribute to inequality and create a digital divide.

Furthermore, gender is a significant factor that determines access to the Internet. This is related to societal and parental perception of gender-based norms, particularly in relation to learning IT. This often leads to the low uptake of science and technology subjects and access to the internet by female students.

3. CHILDREN WHO ARE NOT ONLINE IN SRI LANKA

3.1 Introduction and definitions

Online: According to the Oxford Dictionary, 'online' means, "an activity or service available or performed using the Internet or other computer network". The term can be used to refer to a specific location (e.g. a web page) or to a personal activity. In this document the term 'online' is used to mean that a person is connected to the Internet via a digital device such as a computer, a laptop, a mobile phone, a smart phone or a tablet.

Mobile phones: Three digital devices, standard mobile phones, smart phones and tablets, are referred to as mobile phones in this study.

Computers: Both desktop computers and laptops are identified as 'computers', as survey respondents made no distinction between these devices in their answers.

Digital devices: This term is used to imply both mobile phones and computers (as defined above), unless otherwise specified.

Children: The target groups of this research study were children aged 11-18 years. Unless specifically mentioned, the word 'children' has been used throughout this document to refer to children of both genders.

This chapter provides information on the distribution of children according to their access to the Internet through digital devices. Researchers divided children into the following categories, and administered three separate surveys depending on the category that each child fell into. The third category of children with regular online usage is analyzed in depth.

- a) **Non-IT users:** Children who do not use any digital device. In some cases, digital devices were available at home and schools, but the children were not allowed to use them.
- b) **Non-online-IT users:** Children who have access to a digital device, but have no access to the Internet.
- c) **Online-IT users:** Children who access the Internet and had done so at least once during the 30-day period preceding the date of data collection.

3.2 Distribution of respondents

The majority of children surveyed (52.8 per cent) were online-IT users with regular access to the Internet. Children who used digital devices but did not access the Internet accounted for 39.8 per cent of respondents, and 7.4 per cent were non-IT users who did not use any digital device.

Table 3: Number of children in the different IT user levels, in the government-schools category: by sector, ethnicity and gender

Variable	Non-IT users	Non-online-IT users	Online-IT users	Total
Sample size -----	355	1930	2560	4845
By sector				
Urban -----	59	399	964	1422
Rural -----	260	1462	1531	3253
Plantation -----	32	42	48	122
Not responded -----	4	27	17	48
By ethnicity				
Sinhalese -----	231	1437	1787	3455
Tamil -----	108	347	461	916
Muslim -----	16	143	309	468
Other/ Not responded -----	0	3	3	6
By gender				
Boys -----	138	763	1878	2779
Girls -----	217	1162	681	2060
Not responded -----	0	5	1	6

Figure 4: Distribution of children (11-18 years old), by IT-user levels

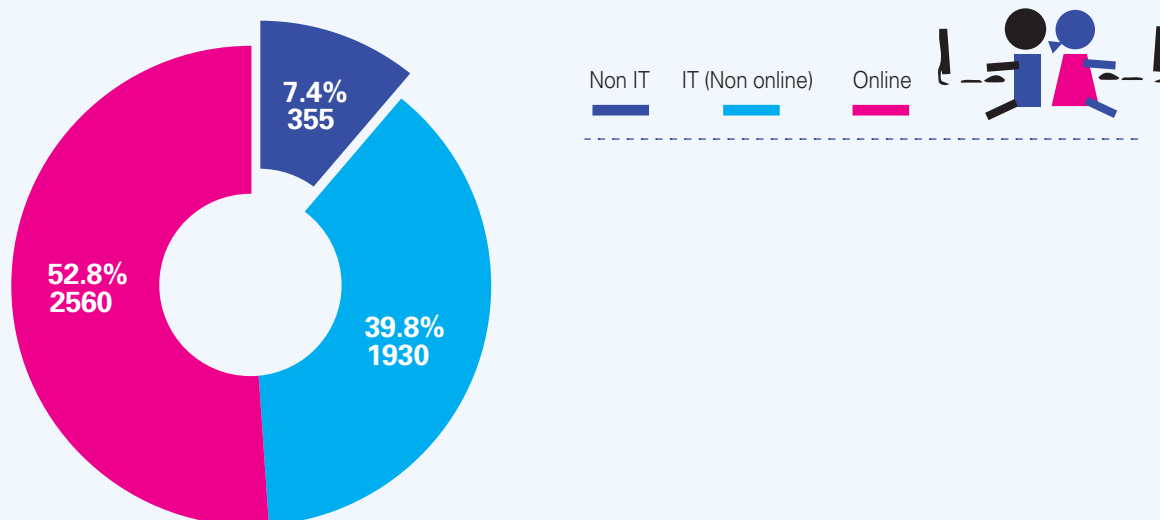
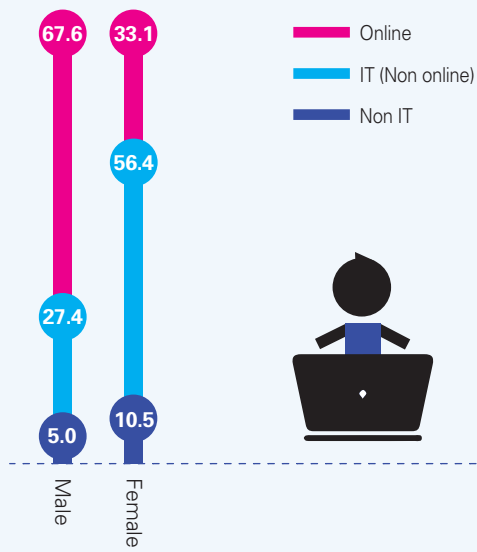
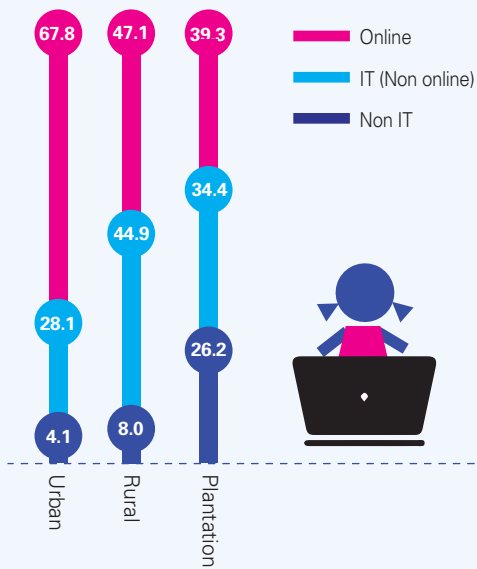


Figure 5: Composition of IT users (as a percentage): by gender



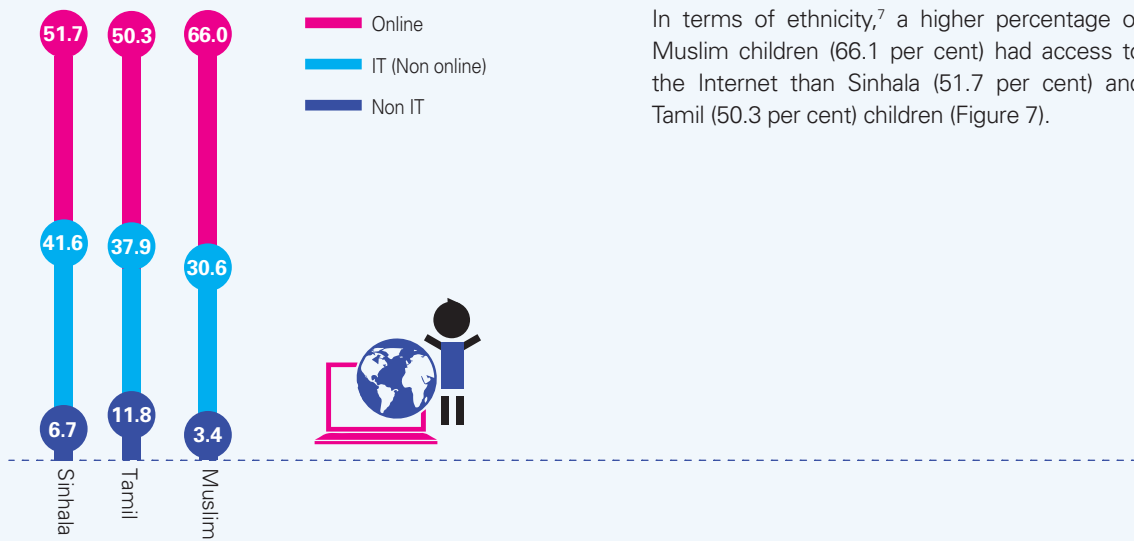
There was a significant gender variation in online-IT users. While 67.6 per cent of boys reported having online access, only 33.1 per cent of girls reported having similar access. In comparison, 56.4 per cent of girls had access to IT, but not to the Internet compared to 27.4 per cent of boys (Figure 5). This situation was confirmed and clarified in the focus group discussions by parents: the majority of girls did not access, or were not permitted to access, the Internet despite having access to digital devices.

Figure 6: Composition of IT users (as a percentage): by sector



Two-thirds (67.8 per cent) of respondents in the urban sector were online users, followed by 47.1 per cent in the rural sector and 39.3 per cent were in the plantation sector (Figure 6).

Figure 7: Composition of IT users (as a percentage): by ethnicity



In terms of ethnicity,⁷ a higher percentage of Muslim children (66.1 per cent) had access to the Internet than Sinhala (51.7 per cent) and Tamil (50.3 per cent) children (Figure 7).

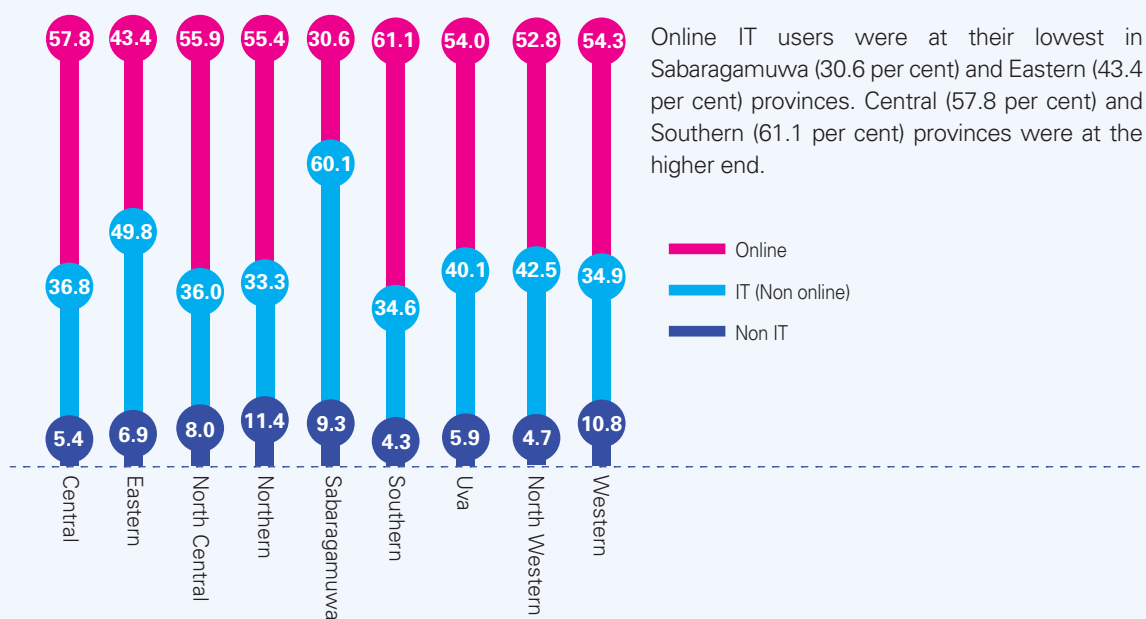
Figure 8: Composition of IT users (as a percentage): by school grades



The lowest numbers of online-IT users were in Grades 6 to 9 (34.9 per cent); online-IT users increased to 58.7 per cent in the Ordinary Level classes and to 70.5 per cent in the Advanced Level classes (Figure 8).

⁷There are three major ethnic groups in Sri Lanka: Sinhalese, Tamil and Muslim. Each group has distinct social and cultural characteristics. Therefore, ethnicity is taken as a variable in this analysis.

Figure 9: Composition of IT users (as a percentage): by province



3.3 Status of non IT users

One of the main reasons for non-use of IT was lack of availability of digital devices. This study found that 79.7 per cent of non-IT users did not have access to computers and 66.4 per cent did not have access to mobile phones. Parental control was another key reason, with 55.7 per cent of non-IT using children reporting that their parents did not allow them to use a mobile phone and 20.3 per cent reporting that parents did not allow them to use a computer. Parent’s inability to afford, either a computer (49.3 per cent) or a mobile phone (31.5 per cent), as reported by children, was another major reason for children not using IT.

It is important to note that a considerable proportion of the children in the non-IT user group reported that they disliked the use of computers (29 per cent) or mobile phones (42 per cent).⁸

Table 4: Reasons for not using a computer or a mobile phone, as expressed by non-IT users

Description	Computer	Mobile Phone
Sample	355	355
I do not have a computer/ mobile phone	283 (79.7%)	236 (66.4%)
I personally do not like to use a computer/ mobile phone	103 (29.0%)	151 (42.5%)
My school does not have a computer lab	19 (5.3%)	-

⁸As focus group discussions were not conducted with non-IT users, it was not possible to ascertain why these respondents disliked the use of computers and mobile phones.

Table 4: Contd.

The use of our school computer lab is restricted to students in a few grades	106 (29.8%)	
My parents do not wish/do not allow me to use a computer/mobile phone	72 (20.3%)	198 (55.7%)
My teachers have advised me not to use a computer/mobile phone	36 (10.1%)	97 (27.3%)
My friends have advised me not to use a computer/mobile phone	26 (7.3%)	33 (9.3%)
My parents cannot afford to buy a computer/mobile phone	175 (49.3%)	112 (31.5%)

Analysis based on multiple responses

3.4 Status of non-online IT users

As shown in Figure 4, 40 per cent of children surveyed were users of digital devices with no access to the Internet. Of this group, 48.3 per cent had access to computers (owned or shared with the family), and 89.4 per cent had access to mobile phones (owned or shared with the family and friends). Computers in the school computer lab were used by nearly half of the non-online-IT users (47.6 per cent); home computers shared within the family were used by about one third (34.3 per cent); and 14 per cent of this group had their own computers but no access to the Internet. Usage of computers at Nenasala telecentres was insignificant at 1.6 per cent.

Table 5: Source of computers and mobile phones used by non-online-IT users

Source of computer	Number	%	Source of mobile phones	Number	%
Own computer	271	14.0	Own mobile phone	323	16.7
Family computer	662	34.3	A family member's mobile phone	1403	72.7
Various other sources (computer of friends, school lab, IT centre, Nenasala, library)	671	34.8	A friend's mobile phone	18	1.0
No access to a computer	326	16.9	No access to a mobile phone	186	9.6
Total	1930		Total	1930	

While using the computers at home (own, family), I also use:		
computers at the school computer lab	919	47.6%
computers at the IT Training Centre	140	7.2%
computers at the Nenasala/Community Centre	30	1.6%

For children with access to a digital device with no Internet, one third of the respondents spent less than LKR 200 per month for mobile phone usage, which was mostly paid by their parents (81.4 per cent). But the largest percentage (40.6 per cent) of this group of children was unaware of how much was spent monthly for usage of the devices.

Table 6: Amount spent per month on mobile phone usage by non-online-IT users

Amount spent per month on mobile phone usage	Number of respondents	%
Less than LKR 200	532	33.2
LKR 200 - 500	320	20.0
LKR 500 - 1000	65	4.0
More than LKR 1000	35	2.2
Not aware	651	40.6
Total	1603	100

Table 7: Source of funds for children's monthly mobile phone bill

Source of funds	Non-online-IT users	
	Number	%
Parents/caregivers	1188	81.4
Friends	9	0.6
Savings	156	10.8
Combination of above three sources	64	4.4
Other	40	2.8
Total	1457	100

3.5 Reasons for not accessing the Internet

This group of non-online-IT users had access to digital devices, yet they did not access the Internet. The major reasons were the lack of a computer with Internet access (43.3 per cent); the lack of a mobile phone/tablet with Internet access (36.4 per cent); and the influence of parents (41.8 per cent) and teachers (11.6 per cent). It is interesting to note that 24.7 per cent of students in Grades 6 to 9, 28.4 per cent in the Ordinary Level classes and 35.5 per cent in the Advanced Level classes reported that it was their personal choice not to access the Internet.

Table 8: Reasons for not accessing the Internet, as expressed by the non-online-IT users

Reason	Total (1930)	Number of respondents		
		Grades 6-9 (986)	Ordinary Level (553)	Advanced Level (391)
I do not have a computer that can access the Internet	836 (43.3%)	421 (42.7%)	252 (45.6%)	163 (41.7%)
I do not have a mobile phone / tablet that can access the Internet	702 (36.4%)	342 (34.7%)	222 (40.1%)	138 (35.3%)
The school computer lab does not have Internet facilities	292 (12.1%)	160 (16.2%)	92 (16.6%)	40 (10.2%)
My family cannot afford to pay for Internet facilities	219 (11.3%)	109 (10.6%)	59 (10.7%)	51 (13.0%)
I cannot afford to obtain Internet facilities provided by IT/Telecentres	159 (8.2%)	96 (9.7%)	44 (8.0%)	19 (4.8%)
My parents do not allow me to use the Internet	807 (41.8%)	438 (44.4%)	233 (42.1%)	136 (34.8%)
My teachers have advised me not to use the Internet	223 (11.6%)	127 (12.9%)	78 (14.1%)	18 (4.6%)
My friends have advised me not to use the Internet	115 (6.0%)	73 (7.4%)	33 (6.0%)	9 (2.3%)
My personal choice	540 (28.0%)	244 (24.7%)	157 (28.4%)	139 (35.5%)

Analysis based on multiple responses

Given that this group of children had access to digital devices but did not access the Internet, researchers explored whether children wanted to have this access. Around two-thirds (68 per cent) of children would like to have access to the Internet, while 17 per cent said that they did not want to have access. More boys (73.3 per cent) than girls (64.7 per cent) said that they would like to have access to the Internet. Younger children, below advanced grade levels, were more likely to want access (68.7 per cent), while 66.1 per cent of advanced grade students said they wanted access. A much higher percentage of children from the plantation sector (71.5 per cent) wanted access to the Internet.

Interestingly, children who do not want access to the Internet were evenly distributed in the urban (17.9 per cent) and rural (17 per cent) sectors, but fewer children in the plantation sector would reject Internet access (7.1 per cent). Higher numbers of girls (19.2 per cent) said that they do not want access compared to boys (13.6 per cent). A quarter of all Muslim children who had access to non-online digital devices said that they do not want access to the Internet.

Table 9: Desire to access the Internet as expressed by the non-online-IT users



Variable	Number of children by response				Total
	Like very much	Like	Undecided	Do not want	
Gender					
Boys	281 37.3%	271 36.0%	99 13.1%	102 13.6%	753 100%
Girls	228 19.8%	518 44.9%	186 16.1%	221 19.2%	1153 100%
Class/Grade					
Below Advanced Level classes	454 29.8%	593 38.9%	222 14.5%	256 16.8%	1525 100%
Advanced Level classes	57 14.8%	198 51.3%	64 16.6%	67 17.3%	386 100%
Sector					
Urban	110 27.7%	150 37.8%	66 16.6%	71 17.9%	397 100%
Rural	379 26.2%	613 42.4%	207 14.4%	245 17.0%	1444 100%
Plantation	13 31.0%	17 40.5%	9 21.4%	3 7.1%	42 100%
Ethnicity					
Sinhalese	394 27.8%	616 43.4%	172 12.1%	237 16.7%	1419 100%
Tamil	80 23.1%	138 40%	78 22.5%	50 14.4%	346 100%
Muslim	34 24.1%	36 25.3%	36 25.3%	36 25.3%	142 100%

4. ONLINE BEHAVIOUR OF CHILDREN IN SRI LANKA

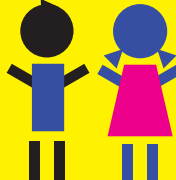
4.1 Introduction

This chapter analyses the behaviour of children who are online. Of the three user categories dealt with in this study, the online-IT-user category was selected for in-depth analysis. The study defined online users as children who had accessed the Internet at least once during the 30-day period preceding data collection.

4.2 Age of first access

Children tended to access the Internet for the first time around the age of 13, irrespective of their ethnicity or gender. Children in the urban sector accessed the Internet about a year earlier, at the age of 12, unlike children from the plantation and rural sectors, which was at 14 years old.

Table 10: Average age of first access of the Internet: by gender, sector and ethnicity

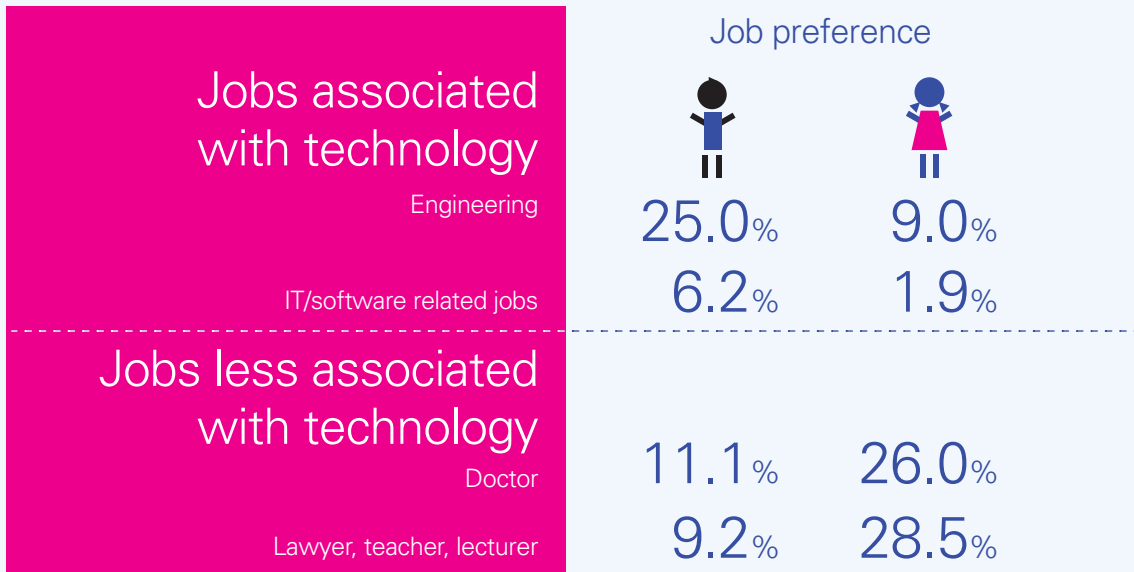
13.1 Boys		Urban	12.7	Sinhalese	13.1
		Rural	14.0	Tamil	13.7
13.6 Girls		Plantation	14.0	Muslim	13.0
Gender		Sector		Ethnicity	

The youngest age of first access of the Internet recorded in the survey was five years old, while the oldest was 18 years old⁹. The study compared children who started using the Internet early (between 5-7 years old) and those who started late (18 years old) to understand the social characteristics of early users and late users. Around three quarters (77 per cent) of the children who began using the Internet at an early age were from the urban sector.

Gender plays a significant role in early access to the Internet. Around 77 per cent of the early users (5-7 years old) were boys, and 75 per cent of the late users (around 18 years old) were girls. It was not possible to ascertain the core factors associated with this gender variation through the survey data from children, but through the data collected from parents, teachers and key informants, it appears that online access and Internet usage for girls was often not prioritized, deterred, or not permitted by adults, leading to reluctance to use the Internet at early ages. Girls in Sri Lanka are not allowed, or they themselves are reluctant, to engage in activities related to technology. Survey data on the career aspirations of children with Internet access lends some credence to this assumption – a higher percentage of boys hoped to get a technology-related job than girls (Table 11). According to traditional norms still prevalent in Sri Lanka, technology is a field regarded as being more appropriate for a boy. This factor may prevent girls using IT devices and accessing the Internet as early as their male counterparts.

⁹The research sample was children who are 11-18 years old.

Table 11: Technology related job preferences by gender



4.3 Devices used for access

Children used mobile phones and computers (some used both) to access the Internet. In government schools, 74.8 per cent of Internet use was through mobile phones and 66.5 per cent of children surveyed used computers to access the Internet. The opposite appears to be true in private schools where more students (80.9 per cent) accessed the Internet using computers. This may be due to the availability of more computers and easy access to IT labs in those schools.

There were also gendered implications on the use of devices. In government schools, 80.2 per cent of boys used mobile phones to access the internet, compared to 75 per cent of girls who used computers. In contrast, in private schools, both genders used computers as their main device to access the Internet.


Muslim children (83.2 per cent) had the highest usage of mobile phones while Tamil (72.9 per cent) children ranked highest for the use of computers. Children in the urban sector used both devices equally to access the Internet, while children in the rural (75.7 per cent) and plantation (70.8 per cent) sectors used mobile phones in much higher numbers for Internet access.

Table 12: Type of digital device used by children to access the Internet: by gender

Gender	Size of sample government schools	Digital device used to access the Internet by children in government schools		Size of sample private & international schools	Digital devices used to access Internet by children in private and International schools	
		Mobile phone	Computer		Mobile phone	Computer
Boys	1,878	80.2%	63.3%	238	67.9%	86.6%
Girls	681	59.7%	75.4%	187	58.8%	73.8%
Total	2,559	74.8%	66.5%	425	64.9%	80.9%

Note: Children who used both devices to access the Internet, were included in both categories

Table 13: Type of digital device used by children in government schools to access the Internet: by ethnicity and sector

Ethnicity and sector	 Sample Size	Digital devices used to access Internet	
		Mobile phone	Computer
Total number of children	2,560	74.8%	66.5%
By Ethnicity			
Sinhalese	1,787	74.7%	66.1%
Tamil	461	69.8%	72.9%
Muslim	309	83.2%	58.6%
Not responded	3	-	-
By Sector			
Urban	964	73.8%	74.0%
Rural	1,531	75.7%	62.0%
Plantation	48	70.8%	60.4%
Not responded	17	-	-

Analysis based on multiple responses




4.4 Source of computers used for access

On average, about one third (37.1 per cent) of children with Internet access used their own computers to go online, with 41.2 per cent of boys and 25.8 per cent of girls owning a personal computer. The majority of the female online-IT users (62.8 per cent) shared a family computer, compared to male (40 per cent). A fair proportion (11.8 per cent) of online-users shared a computer with a friend.

4.5 Internet access through dedicated institutions




School computer labs: According to the study data, computer labs established in government schools did not play a significant role in providing children with access to the Internet. Very few Internet users (11.1 per cent) used the school computer labs. Principals and IT teachers estimated that only about 1.5 per cent of children are able to access their school computer labs on a regular basis.

Table 14: Source of computers used by online-IT users to access the Internet

Source of computers	 (1,878 users)	 (681 users)	 (2,559 users)
I use my own laptop/desktop/tablet	775 41.2%	176 25.8%	951 37.1%
I share a family owned laptop/desktop/tablet	751 40.0%	428 62.8%	1179 46.0%
I share a laptop/ desktop/ tablet with my friend at his/her home	244 13.0%	57 8.4%	301 11.8%
I use a laptop/desktop/ tablet at the school computer lab	188 10.0%	97 14.2%	285 11.1%
I use a laptop/desktop/ tablet at the training institute	79 4.2%	26 3.8%	105 4.1%
I use a laptop/desktop/ tablet at the Nenasala/ community centre/ Internet cafe, etc.	114 6.1%	12 1.8%	126 4.9%

Analysis based on multiple responses

Table 15: Number of online-IT users that accessed the Internet from dedicated institutions

Institution	 (1,878 users)	 (681 users)	 (2,559 users)
School computer lab	188 10.0%	97 14.2%	285 11.1%
IT Training centre	79 4.2%	26 3.8%	105 4.1%
Nenasala/community centre/ Internet cafe and others	114 6.1%	12 1.8%	126 4.9%

Analysis based on multiple responses

Of the 61 government schools that responded, only 42 schools had Internet access. In these 42 schools with Internet connectivity, there was only one computer per 90 students. According to key informant interviews, in most schools, Internet facilities were slow and malfunctioning as there was no regular maintenance and updating. Many schools excluded students from lower grades from accessing the labs due to the lack of time and a heavy focus on classroom learning of the school curriculum.

Table 16: Data on the student population, computer availability and internet access (Grade 6 and above) in government schools

School children population (grades 6 - 13) in 61 schools surveyed	----- 81,976
Number of schools with Internet access	----- 42
Percentage of schools with Internet access	----- 68.8%
Number of children in grades 6 - 13 in the 42 schools with Internet access	----- 65,560
Percentage of children in grades 6 - 13 with Internet access in school	----- 80.0%
Number of computers in the 61 selected schools	----- 1,897
Number of computers with Internet connections	----- 724
Number of computer users in the 61 schools (as per principals' estimates)	----- 1,351
Number of computer users in the 42 schools with Internet access (as per principals' estimates)	----- 1,051
Computer to student ratio (Grades 6-13) in the 61 schools	----- 1:43
Internet access to student ratio (Grades 6-13) in the 42 schools with Internet access	----- 1:90
Percentage of active Internet users in 42 schools	----- 1.6%

Note: Survey of 61 sample schools

As discussed in Chapter 3, nearly half (47.6 per cent) the non-online-IT users said that they used the computers in the school labs. This indicates that school labs generally provided basic access to computers, but not necessarily access to the Internet. In fact, some of the connected schools had computers without online connections in their labs.

There is a push towards improving the state of computer labs in government schools. Some dynamic school principals and IT teachers have secured the necessary support to improve their computer labs and provide an efficient and effective service to their students. The case study presented in Box 1 provides a success story of how the principal and IT teachers of a rural school, located in the Sabaragamuwa Province, improved their school computer lab with the support of national and international donors to meet the IT demands of the children in the area.

Box: 1

Rambuka Maha Vidyalaya a success story

Rambuka Maha Vidyalaya, a national school in a rural setting in the Ratnapura District, has a very active community of IT savvy children who use social media, live-casting and video production, as part of their school work. Their Facebook page, started in 2012, actively engages with 1734 'friends'. News of the school's projects and other selected useful content are regularly updated at least thrice a month. Furthermore, the children also develop video content.

Winning a national IT competition organized by the Ministry of Education in 2004, encouraged the school staff (principal and teachers) to explore IT as a new opportunity. Since then, IT has become a resource driver for the school. They managed to get a computer lab, then an e-village project (in 2009), and other benefits such as video equipment, library books and musical instruments with the support of outside organizations (eg: Karuna Trust Fund) and foreign donors (including expatriates from Australia, Qatar, the UK and the US). Recently, they have received government support to upgrade their computer lab into a larger facility with 67 computers, 40 of which have an Internet connection.

The school has four IT teachers (including IT instructors); two with degree-level IT qualifications. They offer IT education, including in hardware and software, in basic IT, Photoshop, video editing and Internet use. Though they educate children about online security issues in general, it is not included as a separate teaching module. However, the school adopts control systems to screen the websites accessed through its network of computers.

Furthermore, the school offers IT support services to other schools in the area that lack technical support. They offer IT education to the local community in addition to the children.

Students access the Internet both in the school and outside. When outside, they use their mobile phones. Although they were aware of the risks of using the Internet, no one reported abuse. However, the school IT instructor mentioned reports of receiving false email scams (e.g. being declared a lottery winner) and also showed concern that children may share private information with strangers online via their mobile devices.

The 12 parents who were interviewed were aware of the Internet despite not having accessed it personally. Yet, they did demonstrate a reasonable understanding of both the good and bad aspects of the Internet. Among the good aspects, they highlighted the ability to access educational material and also the opportunity to enable their children to be on a par with their urban counterparts. As for the bad aspects, the parents recognized the risks of potential addiction to the Internet and exposure to obscene material. They were vigilant of their children's activities on the Internet, but did not know much about online security. All of the parents wanted to learn more about online security, as they were genuinely concerned about their children's safety.

Nenasala and IT training centres: IT centres, including Nenasala, have been set up in rural areas and in townships by government and non-governmental entities. From the perspective of 'inclusiveness' and 'digital divide', they fill a gap in the rural sector where children do not have IT facilities and offer an opportunity for computer literacy, and for additional IT training to those who want to take IT courses and obtain an external certificate for a fee. A few children tended to collect these additional technical qualifications while in school, as they believed such certificates will add value at job interviews after completing their school career.

However, according to the survey, institutions such as Nenasala and IT centres play a minimal role in terms of serving IT users who are online. Only 4.9 per cent of online-IT users accessed the Internet on computers at these institutions (Table 13), confirming that the institutions mostly served the non-online-IT users to become computer literate, but not necessarily to access the Internet. Of the few children with Internet access who used centres such as Nenasala 6.1 per cent were boys and a mere 1.8 per cent were girls (Table 15).

4.6 Sources of income for access

Two thirds of the respondents spent less than LKR 500 per month on mobile phone usage and 55.6 per cent spent a similar amount on Internet access. Based on the multiple answers provided by the users, it is clear that for nearly two thirds of the respondents, the cost was borne by the family (mostly parents). It is important to note that one third of children with access to the Internet said that they paid the cost from their savings.

Table 17: Monthly expenditure on mobile phone and Internet usage by online-IT users

Amount per month (LKR)	Mobile phones		Internet	
	Number	Percentage (%)	Number	Percentage (%)
Less than 200	933	41.5	799	33.4
200 - 500	522	23.2	531	22.2
500 - 1000	196	8.7	248	10.4
More than 1000	92	4.1	230	9.6
Not aware	504	22.5	582	24.4
Total	2,247	100	2,390	100

Table 18: Source of funds to pay for mobile phone and Internet bills

Source of funds	Mobile phones (2,247)	Internet (2,390)
Parents/caregivers/relations	1,439 (64.0%)	1,649 (69.0%)
Friends	53 (2.4%)	49 (2.0%)
My savings	811 (36.1%)	795 (33.3%)
Other	80 (3.5%)	138 (5.8%)

Analysis based on multiple responses

4.7 Frequency of access

Half the respondents in the group of children who had Internet access went online at least once per day, with 28.7 per cent accessing the Internet more than once daily. Another 30 per cent of the online-IT users accessed the Internet 2-3 times per week, while 19.1 per cent did so only 2-3 times per month (Table 19).

A higher percentage of boys (56.2 per cent) accessed the Internet at least daily compared to 35.7 per cent of girls. Children in the urban sector accessed the Internet more frequently than children in the rural and plantation sectors.

Table 19: Frequency of children accessing the Internet: by gender, sector, ethnicity, grade & province

	Frequency				Total
	More than once per day	Once per day	2-3 times per week	2-3 times per month	
By gender					
Boys	631 34.0%	413 22.3%	522 28.1%	289 15.6%	1,855 100%
Girls	89 13.7%	143 22.0%	230 35.3%	189 29.0%	651 100%
Total (Boys and Girls)	720 28.7%	556 22.2%	752 30.0%	478 19.1%	2,506 100%
By sector					
Urban	317 33.6%	230 24.4%	265 28.2%	130 13.8%	942 100%
Rural	389 26.0%	314 20.9%	467 31.1%	331 22.0%	1,501 100%
Plantation	8 17.0%	8 17.0%	17 36.2%	14 29.8%	47 100%
By ethnicity					
Sinhalese	508 29.2%	387 22.2%	505 29.1%	337 19.4%	1,737 100%
Tamil	106 23.1%	96 20.9%	158 34.4%	99 21.6%	459 100%
Muslim	102 33.7%	72 23.8%	87 28.7%	42 13.9%	303 100%
By grade					
Grades 6 - 9	150 23.5%	144 22.5%	225 35.2%	120 18.8%	639 100%
Ordinary Level	218 23.9%	199 21.8%	291 31.9%	205 22.4%	913 100%
Advanced Level	352 68.8%	213 22.3%	522 28.1%	237 24.8%	956 100%

Table 19: Contd.

	Frequency				Total
	More than once per day	Once per day	2-3 times per week	2-3 times per month	
By province					
Central	132 32.5%	71 17.5%	125 30.8%	78 19.2%	406 100%
Eastern	45 25.4%	46 26.0%	46 26.0%	40 22.6%	177 100%
North Central	49 33.8%	25 17.2%	45 31.0%	26 17.9%	145 100%
Northern	66 24.8%	64 24.1%	86 32.3%	50 18.8%	266 100%
Sabaragamuwa	32 20.8%	35 22.7%	52 33.8%	35 22.7%	154 100%
Southern	99 27.8%	77 21.6%	104 29.2%	76 21.3%	356 100%
Uva	29 16.0%	45 24.9%	62 34.2%	45 24.9%	181 100%
North Western	113 28.3%	90 22.6%	129 32.3%	67 16.8%	399 100%
Western	155 36.5%	103 24.5%	104 24.5%	62 14.6%	424 100%

4.8 Learning how to access the Internet

Most of children with Internet access (53.6 per cent) had taught themselves how to use the Internet. While 60.3 per cent of boys were self-taught, nearly half of the girls had been taught by their siblings, likely their brothers (Table 20). These trends were not significantly different among the ethnic groups. The social norm of encouraging boys to engage in technology within the context of career aspirations in the IT field has led to boys improving their IT skills and competencies. Boys acquired the capacity and permission for self-learning while girls were taught computer applications by siblings. Among all three ethnic groups, the primary mode of learning to use the Internet was self-learning followed by learning from siblings.

Table 20: Mode of learning to access and use the Internet: by gender and ethnicity

"Who taught you to use the Internet?"	Gender		Total (2,559)	Ethnicity		
	Boys (1,878)	Girls (681)		Sinhalese (1,787)	Tamil (461)	Muslim (309)
Self-taught	1,134 60.3%	239 35.1%	1,373 53.6%	999 56%	199 43.2%	170 55.0%
My parents	249 13.2%	174 25.6%	423 16.5%	276 15.4%	93 20.1%	50 16.2%
My siblings	556 29.6%	322 47.3%	878 34.2%	587 32.9%	174 37.7%	113 36.6%
My teacher/ trainer	311 16.5%	146 21.4%	457 17.8%	337 18.9%	74 16.0%	44 14.2%
My friends	604 32.1%	114 16.7%	718 28.0%	503 28.2%	119 28.8%	94 30.4%
My relations	252 13.4%	109 16.0%	361 14.1%	218 12.2%	82 17.8%	62 20.1%

Analysis based on multiple responses

4.9 Reasons for accessing the Internet

Children reported different reasons for using the Internet, with the top reasons being to: search for educational information (86.2 per cent); download information/software/videos, (71.8 per cent); watch films/YouTube/videos (60.8 per cent); use social media (60.3 per cent); listen to music/radio (55.5 per cent); and play online games (54.4 per cent).

Searching for information is the major reason for accessing the Internet. Most of the respondents (86.2 per cent) accessed the Internet to search for educational information, very likely for their studies with a higher percentage of girls (92.1 per cent) reporting this type of usage. Of the respondents, 71.8 per cent accessed the Internet to download items, and it is possible that some of this content may have also been used for educational purposes. Children accessed the internet to watch online content including films, YouTube and videos (60.8 per cent), an activity more popular among girls (56.5 per cent) than boys (62.4 per cent). A similar percentage (60.3 per cent) of children engaged in social media, although this time with higher number of boys (65.8 per cent) than girls (45.1 per cent). Listening to music/radio was another popular activity, equally engaged in by boys (55.9 per cent) and girls (54.3 per cent). Playing online games, engaged in by 54.4 per cent, was far more popular among boys (60.2 per cent) than girls (38.5 per cent). These patterns of Internet usage were not markedly different by ethnicity or sector. It is also noteworthy that, unlike adults, sending emails was not a popular activity among children.

Table 21: Reasons why children access the Internet by gender, ethnicity and sector

Purpose	Total (2,559)	Gender		Ethnicity		
		Boys (1,878)	Girls (681)	Muslim (309)	Sinhalese (1,787)	Tamil (461)
Search for educational information	86.2%	1,581 84.1%	627 92.1%	269 72.9%	1,512 84.7%	422 91.5%
Send emails	28.3%	569 30.3%	156 22.9%	90 24.4%	192 10.8%	139 30.2%
Use social media	60.3%	1,237 65.8%	307 45.1%	220 59.6%	1,030 57.7%	289 62.7%
Watch films/ YouTube/ videos	60.8%	1,172 62.4%	385 56.5%	185 50.1%	1,062 59.5%	305 66.2%
Share photos/ videos	34.8%	740 39.4%	151 22.2%	126 34.1%	586 32.8%	174 37.7%
Listen to music/ radio	55.5%	1,050 55.9%	370 54.3%	164 44.4%	1,000 56.0%	252 54.7%
Play online games	54.4%	1,131 60.2%	262 38.5%	190 51.5%	905 50.7%	294 63.8%
Watch sports	34.8%	793 42.2%	98 14.4%	146 39.6%	562 31.5%	180 39.0%
Download information/ software/ videos, etc.	71.8%	1,396 74.3%	443 65.1%	216 58.5%	1,287 72.1%	332 72.0%
Engage in online window shopping	30.9%	665 35.4%	126 18.5%	103 27.9%	571 32.0%	114 24.7%
Chat with boy/ girl friend, relations & friends	40.7%	851 45.3%	192 28.2%	158 42.8%	684 38.3%	200 43.4%

Analysis based on multiple responses

Table 21: Contd.

Purpose	Sector		
	Urban (964)	Rural (1,531)	Plantation (48)
Search for educational information	837 86.8%	1,313 85.8%	44 91.7%
Send emails	337 35.0%	368 24.0%	16 33.3%
Use social media	639 66.3%	870 56.8%	23 47.9%
Watch films/ YouTube/ videos	660 68.5%	856 55.9%	32 66.7%
Share photos/ videos	390 40.5%	472 30.8%	22 45.8%
Listen to music/ radio	570 59.8%	821 53.6%	26 54.2%
Play online games	600 62.2%	755 49.3%	31 64.6%
Watch sports	400 41.5%	473 30.9%	14 29.2%
Download information/ software/ videos, etc.	714 74.1%	1077 70.3%	38 79.2%
Engage in online window shopping	368 38.2%	407 26.6%	9 18.8%
Chat with boy/girl friend, relations & friends	456 47.3%	568 37.1%	13 27.1%

Analysis based on multiple responses

4.10 Frequently accessed websites, apps and social media

Using web analytics (eNovation4D Ltd., 2015), this study analyzed internet usage in Sri Lanka broadly. An analysis of the top 20 site rankings shows that Facebook is the top accessed site in the country. The Internet is also becoming a popular source of information and medium of education in Sri Lanka. Wikipedia is ranked 15th among the top 20 most popular websites in Sri Lanka, and search engines such as Google and Yahoo are also top ranked. Social media and social networking capture the biggest online visitor audience in Sri Lanka. Twitter.com also ranks among the top 20 popular sites.

Table 22: Top-20 most popular websites and apps of the Sri Lankan public

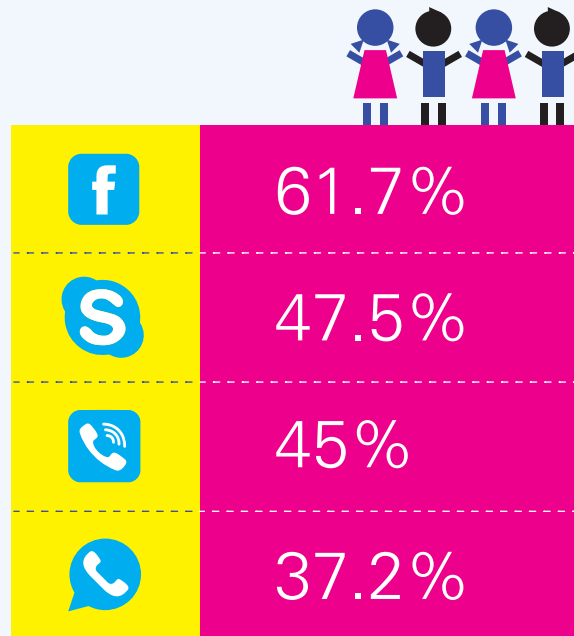
Rank	Name of the Website/App	Type of service
1	Facebook.com	Social media
2	Google.com	Information search / search engine
3	Google.lk	Information search / search engine
4	Youtube.com	Online video site
5	Blogspot.com	Information / social media
6	ikman.lk	Online buy and sell site / e commerce site
7	Hirufm.lk	Radio and music online
8	Yahoo.com	Information search
9	Gossi plankanews.com	Gossip site
10	Amazon.com	e commerce site
11	Ebay.com	e commerce site
12	Hirunews.lk	News site
13	Lankadeepa.lk	News site
14	Adaderana.lk	News site
15	Wikipedia.org	Online encyclopedia
16	Ask.com	Information search / search engine
17	Nethfm.com	News site
18	Twitter.com	Social media
19	Espncricinfo.com	Sports news site (Cricket)
20	Xhamster.com	Adult video and dating site

Source: Top sites in Sri Lanka, Alexa. www.alexa.com. 23rd August, 2015.

Only three e-commerce sites, Ikman.lk, Amazon.com and Ebay.com, are among the top 20 sites. Having Ikman.lk ranked 6th, ahead of Amazon and Ebay, suggests that most of the e-commerce is taking place within the country. Among the top 20 sites, only one is known for adult content (Xhamster.com, ranked 20th).

The above information of the popular sites (including apps) covers the total population of the country, including adults. According to children's responses in this study, four major social media sites/apps were popular among children:

Facebook, the most popular social media site among children, was more popular among boys (72 per cent) than girls (33.1 per cent) and generally, a higher percentage of boys accessed social media compared to girls. Children's access of websites and apps varied between Ordinary Level and Advanced Level students, between students of different schools, and between boys and girls. The data gathered from focus group discussions with children (Ordinary and Advanced Level students) revealed that Facebook, You Tube, ikman.lk, Google were their preferred sites.



Viber and Skype were accessed by a higher percent of Tamil children (59 per cent and 62.7 per cent respectively) compared to Muslim (57.3 per cent and 51.8 per cent respectively) and Sinhalese children (29.4 per cent and 42.8 per cent respectively). On the other hand, WhatsApp was accessed by a higher percentage of Muslim children (72.8 per cent) compared to Tamil (39.9 per cent) and Sinhalese children (30.4 per cent).

Figure 10: Percentage of children using social media and apps: by gender, ethnicity and sector

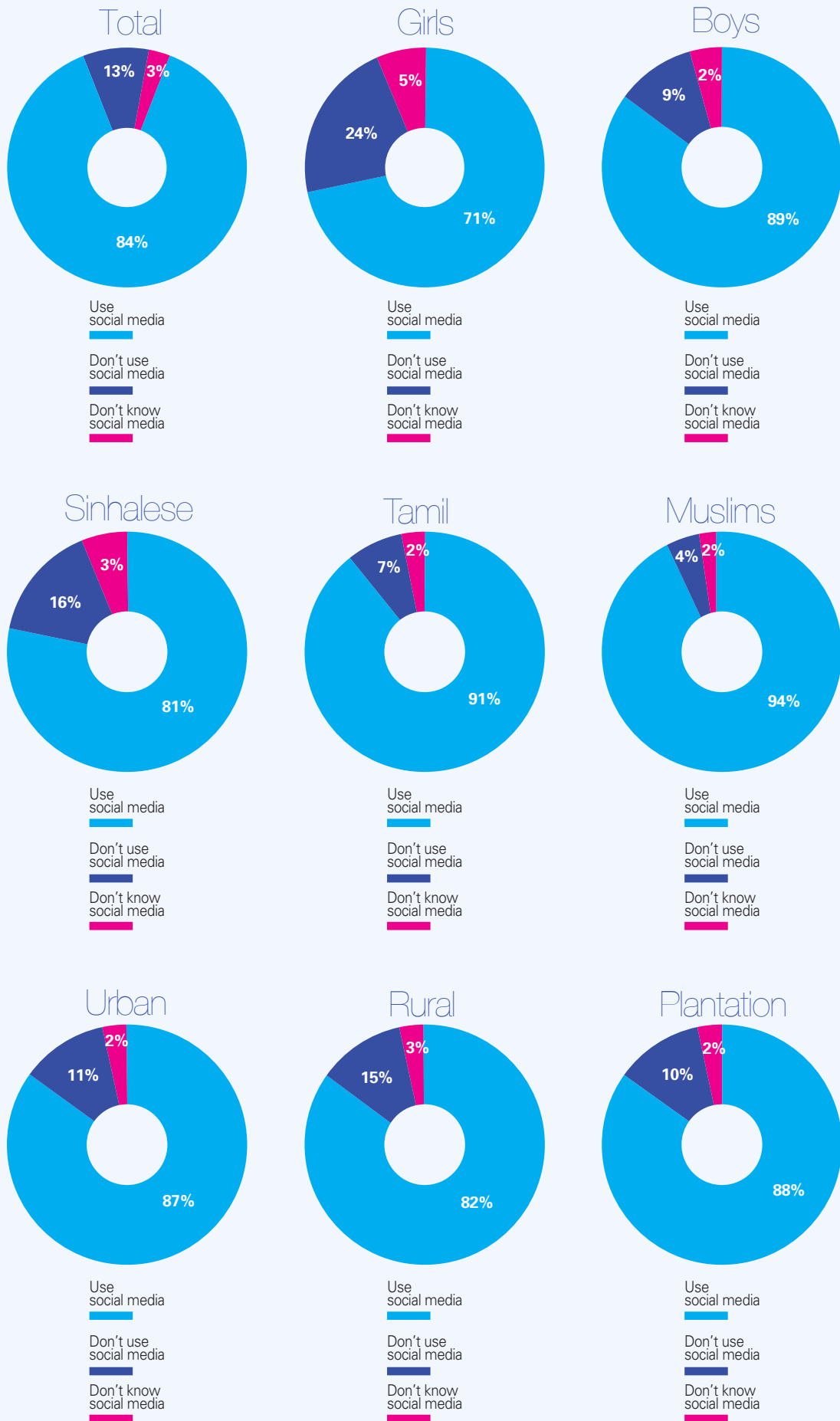


Figure 10.1: Percentage of children using social media and apps: by school, grade and province

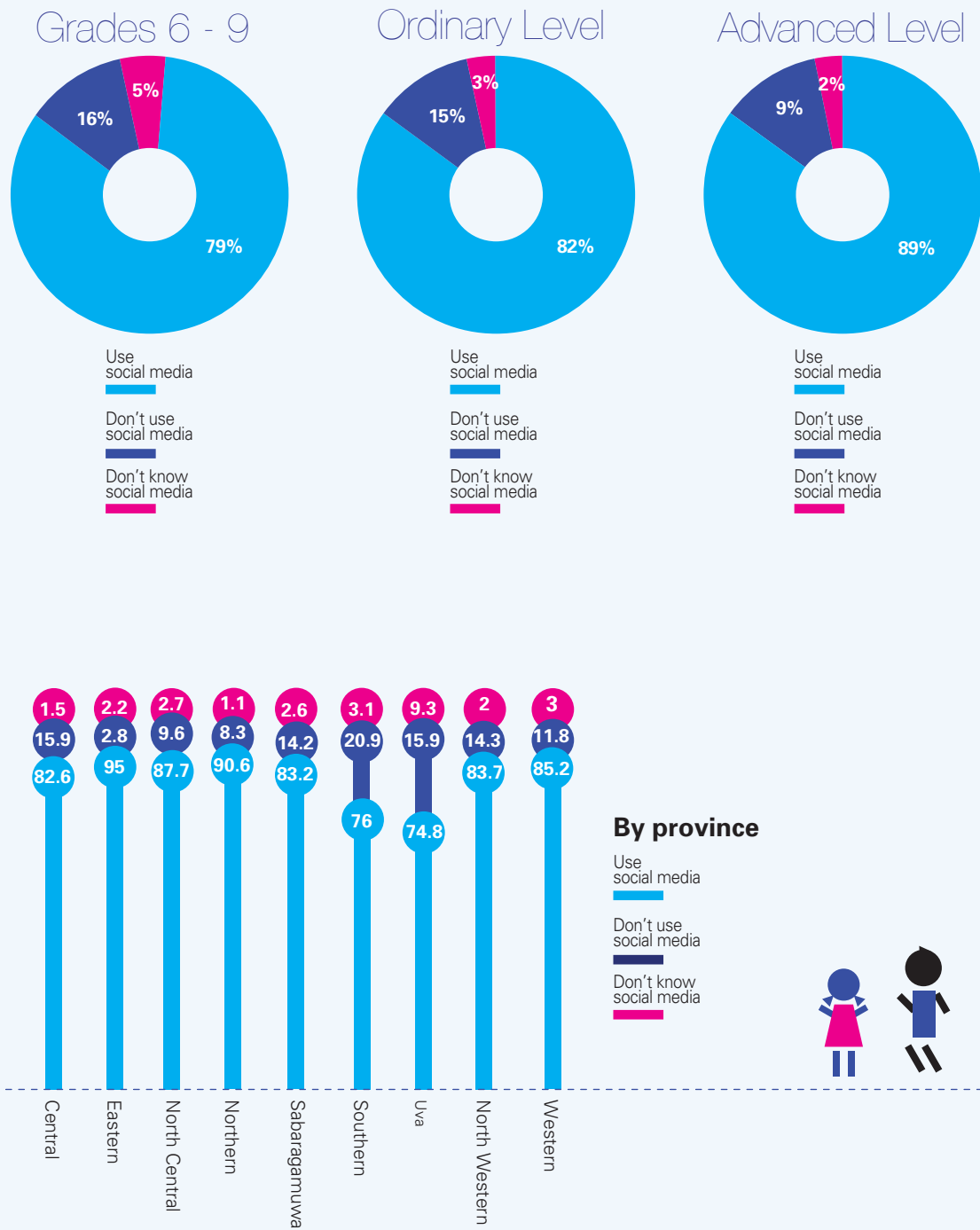


Table 23: Websites and apps accessed by children: by gender and ethnicity

Social media networks accessed	Total (2,559)	Gender		Ethnicity		
		Boys (1,878)	Girls (681)	Sinhalese (1,787)	Tamil (461)	Muslim (309)
Viber	45.0%	48.4%	35.5%	29.4%	59.0%	57.3%
Skype	47.5%	50.0%	40.6%	42.8%	62.7%	51.8%
Facebook	61.7%	72.0%	33.1%	63.1%	62.5%	52.1%
Twitter	20.3%	24.2%	9.7%	18.4%	25.2%	23.9%
Flickr	1.9%	2.4%	1.0%	1.6%	3.2%	1.6%
Twoo	1.4%	1.7%	1.0%	1.2%	1.7%	1.9%
WhatsApp	37.2%	41.3%	25.8%	30.4%	39.9%	72.8%
Instagram	12.7%	15.7%	4.2%	10.7%	16.7%	17.5%
Snapchat	2.1%	2.5%	1.0%	1.5%	4.1%	1.9%
Tumblr	1.1%	1.1%	1.3%	1.2%	0.9%	1.0%
Kik	1.9%	2.6%	0.0%	1.8%	2.2%	1.9%
Wechat	5.0%	5.8%	2.6%	2.7%	9.3%	11.3%
Google Plus	5.7%	5.6%	5.7%	6.9%	2.8%	1.3%

Table 23.1: Websites and apps accessed by children: by Grade

Social media networks accessed	Grade		
	Grades 6 - 9 (658)	Ordinary Level (923)	Advanced Level (979)
Viber	35.9%	43.0%	53.1%
Skype	44.8%	48.3%	48.5%
Facebook	44.8%	62.0%	72.6%
Twitter	14.3%	20.2%	24.5%
Flickr	1.5%	1.7%	2.3%
Twoo	1.8%	1.2%	1.3%
WhatsApp	26.7%	35.5%	45.9%
Instagram	7.1%	10.5%	18.3%
Snapchat	0.6%	1.9%	3.3%
Tumblr	1.1%	1.0%	1.3%
Kik	2.3%	1.2%	2.3%
Wechat	4.2%	4.9%	5.5%
Google Plus	4.4%	4.9%	1.6%

Figure 11: Percentage of access to social media/apps: by gender

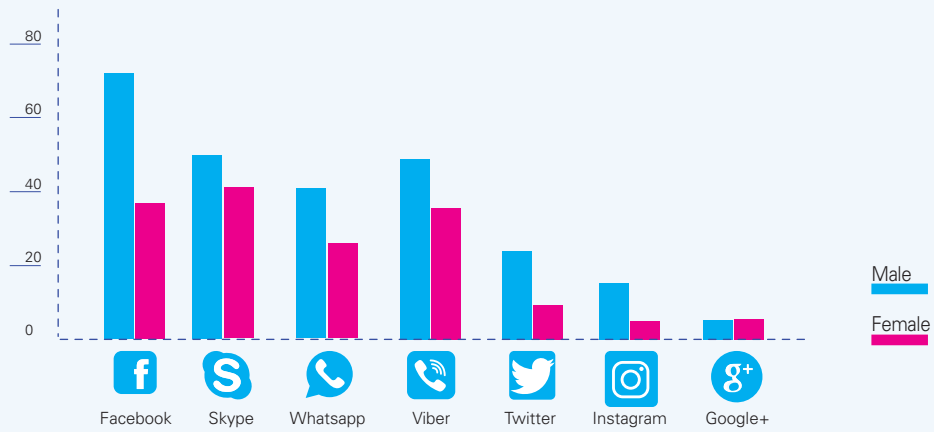


Figure 12: Percentage of access to social media and apps: by grade

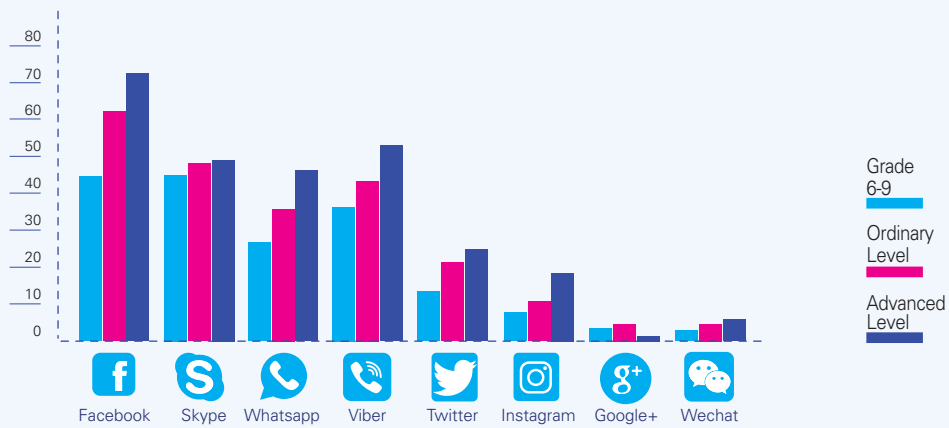


Figure 13: Percentage of access to social media and apps: by ethnicity

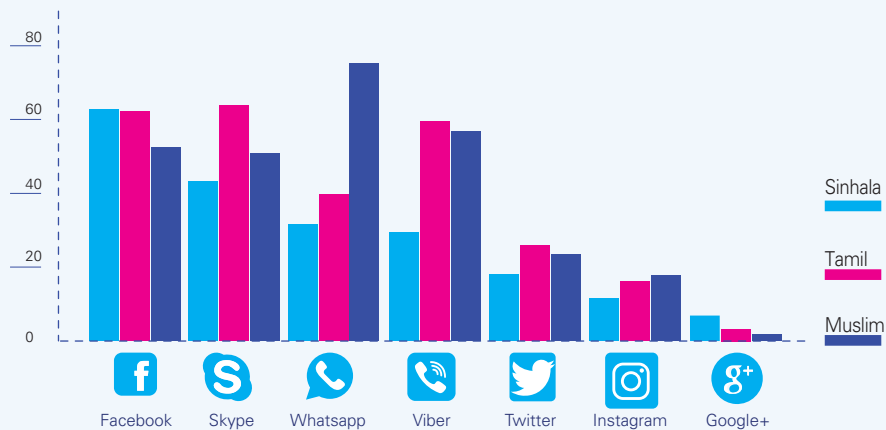


Table 24: Frequently accessed sites/apps by adolescents, especially in grades 10-12¹⁰

Type of school and sector	Sites accessed by school children (number of responses/total respondents)
Girls' schools (Sinhala) Colombo - urban	Facebook.com (13/16); game.lk (11/16); lkman.lk (11/16); Ananmanan.lk (10/16); Instagram (05/16); E-buy (05/16); Topsinhala.lk (01/16); Hitad.lk (01/16); Idealbeep.lk (01/16); Gossip Lanka(01/16) Youtube, Clip Converter, Google, Wiki, Drama V
Girls' schools (Sinhala) Kurunegala - urban	Facebook (6/8); Youtube(5/8); Wikipedia (3/8); ebooks/wrox.com (1/8); ebay(4/8); Webopedia(1/8); Mini clips (2/8); Knorr - cooking recipes (1/8); W3schools (5/8); Hirugossip (2/8); geekcodes(1/8); dailymotion(3/8)
Girls' schools (Sinhala) Kandy - urban	Youtube; Wikipedia; Google; encyclopedia; Edu Lanka;
International schools Colombo - urban	Facebook; Youtube; Wikipedia; Google; ebay; MP4.ee; MP3Skull; downloader; Wikipedia (3/7); Crunchyroll (1/7); Watchop.com (1/7); Couch tuner (1/7)
Mixed schools (Sinhala) Galle - rural	DJ lanka; sinhalalanka; gossiplanka; Xhamster.com; phonerotica.com; begcy.com; srilankaxxx.videos; ananmanan; wabdab; e-bay; ikman.lk; biscop.lk; elakiri.lk; school.lk; wabtrick; atspot.lk; lightxxx.com; brazzer.com;
Mixed schools (Sinhala) Anuradapura - rural	Sinhalalanka.com; ananmanan.lk; jayasrilanka.com; ikman.lk; waptrick.com; beeg.com; 3Gpvideo.com; 95.com; ethakshalawa.lk; NVQ.com; donex.lk; hiru TV.lk;
Mixed schools (Sinhala) Hambantota - rural	Youtube; Jayasirilanka.net; ikman.lk; elakiri.com; google.com, 89.com; porntube.co; brazzers.com; redwap.com; red pussy.com; wap95.com; naughtyamerica.com;
Mixed schools (Sinhala) Ratnapura - urban	Ananmanam.lk; sinhalalank.com; srilankacodes.lk; gossip.lk; Hirutv.lk; callthree.com; srilankagirl.com; love tips; hotgirls.com; hotgossip.com;
Mixed schools (Tamil) Kilinochchi - rural	Facebook; Wikipedia; Amazon; Google; lkman; Espn; Lankasri; Uthayan; Yahoo - Education Sites, Sports, News, E-commerce;
Mixed schools (Tamil) Nuwara Eliya - plantation	Youtube; lkman; kutyweb; Wikipedia; tailkey

¹⁰A number of respondents, in some schools, was not available

Children's most common uses of the social media (Facebook, in particular) were to find relationships, keep up with friends, chat with friends and find new friends. There was a fair number of children with access to the Internet (17 per cent) who used Facebook to engage in online-shopping activities, as Facebook is widely used for various product promotions. Both genders engaged in all these activities with boys being more active. Furthermore, it is clear that the majority of online activities on social media were related to downloading, viewing and learning. Uploading and sharing comments, photos and videos were done only by 72.4 per cent of the Facebook users.

The Ministry of Education established an educational web-site called e-thaksalawa in all three languages (Sinhala, Tamil and English), which provides educational material, curricula and other related information for children in primary and secondary schools. However, only 15.2 per cent of children in the sample had accessed this site, even those using school computers as their primary internet access point.

4.11 Children's online interactions

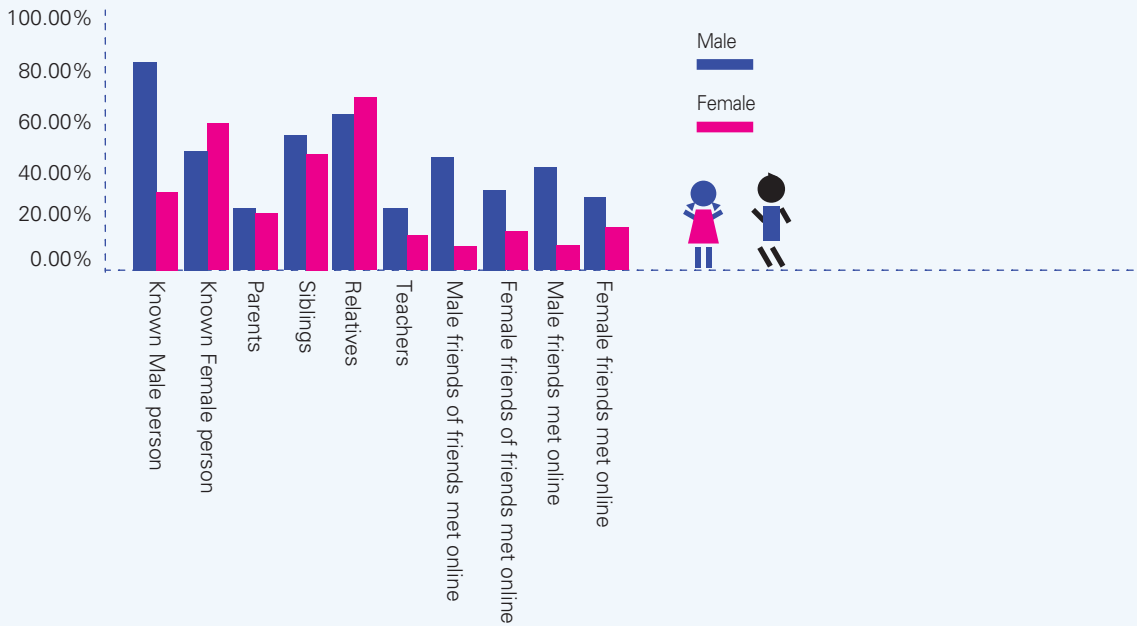
Children used social media to communicate with known persons. They also communicated with people that they had met online but had never met in person. Known people included friends, parents, relatives, teachers and siblings. Children communicated most frequently with relatives who lived overseas or lived in distant places in the country. In Sri Lanka today, dispersed families are common, and in many cases, children live in boarding facilities and hostels, parents may reside away from home for work, and parents and relatives live overseas. Some children reported that they used applications such as Skype, Viber and WhatsApp, to carry out live, online conversations, send text-based messages, photographs, and videos to keep in touch with family members they could not meet regularly in person. Siblings also communicated with each other and shared material on their common social interests through these apps. Children reported in focus group discussions that the physical gap between family members and relatives was bridged to some extent through these online tools.

Table 25: Reasons for using Facebook, as expressed by children with Internet access by gender & ethnicity

Reason	Boys (1,353)	Girls (226)	Sinhalese (1,127)	Tamil (288)	Muslim (161)
To become aware of friends' activities	77.7%	66.8%	78.8%	73.2%	66.4%
To chat with friends	84.8%	64.6%	83.7%	76.3%	78.9%
To share comments/ updates/ upload photos/ videos	75.1%	55.7%	74.0%	83.8%	72.7%
To find/add new friends	67.1%	33.6%	63.3%	57.6%	62.7%
To become aware of upcoming events	50.7%	32.3%	42.9%	57.6%	65.2%
For sourcing products and services for sourcing products and services (by Facebook users) ¹¹	18.2%	10.2%	16.9%	12.8%	24.8%

Analysis based on multiple responses

Figure 14: Individuals that children communicated with online: by gender



Children used social media to communicate mostly with known people such as parents (23.8 per cent), siblings (50.3 per cent), relatives (61.3 per cent) and teachers (21 per cent). However, a significant proportion of online users (46.3 per cent), also communicated with unknown persons that they had met online. Children increased the number of male and female ‘friends’ in their social networks through social media, and these were mostly ‘online first friends’ and acquaintances that they had loose connections to in real life. The percentage of boys who communicated with both genders is much higher than that of girls.

A higher percent of Tamil children (72.6 per cent) used social media to communicate with their relatives compared to Sinhalese (56.5 per cent) and Muslim (69.6 per cent) children.

¹¹Table 21 shows that 30.9 per cent of children are engaged in e-shopping using social media/apps; 17 per cent represent those who shop through FB.

Table 26: Persons with whom children communicate using social media: by gender, ethnicity and sector

Persons children communicate with	Boys (1668)	Girls (483)	Sinhalese (1,438)	Tamil (420)	Muslim (290)	Urban (837)	Rural (1,256)	Plantation (42)
Known persons								
Known boys	80.4%	29.6%	74.3%	54.8%	62.8%	70.8%	68.1%	59.5%
Known girls	45.9%	56.3%	53%	41.7%	43.4%	54.6%	46.8%	38.1%
Parents	24.3%	21.9%	19.1%	26.7%	13.1%	29.7%	20.3%	21.4%
Siblings	52.0%	44.7%	51.5%	42.6%	56.5%	52.4%	49.8%	40.5%
Relatives	59.9%	66.0%	56.5%	72.6%	69.6%	66.4%	58.2%	57.1%
Teachers	23.2%	13.2%	19.5%	22.1%	26.5%	23.3%	19.5%	28.6%
Unknown persons								
Male friends of friends met online	44.4%	9.1%	39.7%	24.8%	36.5%	38.8%	35.1%	26.2%
Female friends of friends met online	31.0%	14.9%	31.3%	17.3%	22.1%	30.6%	25.5%	21.4%
Male friends met online	39.8%	9.1%	35.9%	20.2%	35.9%	26.6%	31.8%	26.2%
Female friends met online	28.2%	16.3%	28.8%	15.9%	23.1%	34.9%	25.0%	19.0%

Analysis based on multiple responses

4.12 Positive Online Experiences

Children said that there were a range of benefits of being online. They accessed the Internet to check their examination results upon their release, instead of waiting anxiously to receive them by post. Most children, with little gender variation, regarded accessing their examination results online (56.4 per cent) as their first memorable online experience. Other important benefits were reading e-books (28.2 per cent), followed by uploading their own creations such as stories, poems, and presentations (22.5 per cent), submitting academic work (14.8 per cent), and identifying a school or university to pursue their education or to take a course (12.2 per cent) and 10 per cent had discovered ways to plan cost-effective trips. Interestingly, 10.9 per cent of the boys were able to find a girlfriend on the Internet (this was among older students).

Two case studies of high-frequency Internet users are presented in Box 2 and Box 3. These two case studies show that there was a gender variation in relation to online behavior. Girls, though they were heavy users, took necessary precautions to reduce online risks, while boys were not only vulnerable, but also became involved in risky actions.

Box: 2

**A profile of a high-frequency Internet user:
A student from an Advanced Level class in an urban girls' school**

K is a 17 year old Sinhalese girl studying for her Advanced Level examination (arts) in the English medium. Her father is a businessman and her mother is a school teacher. She aspires to be a university lecturer, and uses a computer for her school work and also owns a smart phone. Her monthly mobile phone bill is less than Rs.200, which she settles with the money she gets from a friend.

K doesn't use the school computer to access the Internet. Although she uses the computer at home to go online, she doesn't know what it costs as the monthly bill is paid by her parents. She started accessing the Internet when she was 10 years old. She taught herself how to access the Internet and does so several times a day for a variety of purposes, including to search for education opportunities, send emails, watch films, sports and videos, share photos, listen to music, play games, download a variety of materials, search for gossip, engage in e-commerce activities, chat with friends, write blogs and update her website.

K regularly uses social media including Viber, Twitter, WhatsApp, Instagram, Snapchat, Tumblr and chats on Skype with her friends. She comments, uploads photos and videos, and has found new friends through Instagram and Tumblr. She finds upcoming events using Twitter. She communicates with her teachers, parents, siblings and relatives, as well as unknown people (both male and female) she has met online.

K does not give her personal information to unknown people and ignores such requests. She has never physically met anyone she got to know online. Yet, she has accepted chat requests from unknown people. From time to time, she changes her social media privacy settings. She has received false messages informing her that she has won a lottery. Once someone had hacked her password and her profile, which was an upsetting incident; she informed her parents and later changed her password. She said that when she browses the Internet, pictures that are more suitable for adults have popped up on her screen, many times.

At present, she learns from her teachers, parents, mass media and websites how to protect herself when using the Internet. She always tells her parents what she does on the Internet, and her parents are also watchful of what she is doing. She has never received any training on online security, but she said it will be very useful for children.

K says that children and youth should use the Internet to be successful in life. She said she really feels bad when she doesn't get to access the Internet. Memorable features of her online life so far have been the completion of an online exam and checking for her Ordinary Level examination results. Although K is a regular online user and is aware of e-thaksalawa (the website of the Ministry of Education), she has not used the website.

Box: 3

A profile of a high-frequency Internet user: A boy from an Advanced Level class in an urban-mixed school

S is a 17 year old Sinhalese boy studying for his Advanced Level (commerce) examination in the Sinhala medium in a mixed school in the Colombo District. He also takes an IT course at an IT training institute. His father is a private company manager and his mother is a housewife. He aspires to become a pilot.

He owns a smart phone and draws on his savings to settle the monthly bill, which exceeds Rs 1,000. He uses his own computer at home and had started accessing the Internet with his smart phone when he turned 17 years old. Self-taught, he accesses the Internet several times a day to search for educational opportunities, send emails, watch films, videos and sports, share photos, listen to music, play games, download a variety of materials, search for gossip, engage in e-commerce activities, chat with friends, write blogs and update his website.

He regularly uses Viber, Facebook, WhatsApp, Instagram, Snapchat and Kik, and also Skype, to chat with friends. He uses Facebook to chat with his friends, share comments, upload photos, find new friends, learn about upcoming events and for e-shopping activities.




S communicates through social media with friends, siblings, relatives, friends of friends he has met online, as well as unknown males and females. However, he does not communicate with his parents and teachers through social media. He physically met one person he had met on the Internet, who later became his girlfriend. Before the meeting, he informed one of his friends, but not his parents, that he was going to meet her. He has changed his privacy settings several times as a safety measure.

He admits that he has sent nasty e-mails and messages to hurt the feelings of others. He, too, has received embarrassing pictures and photos to his account and threats from unknown persons. He also receives pictures and videos with adult content. He does not know to whom he should complain when such incidents happen.

S has never received any training on online security. He said friends and websites were the best means to learn how to be safe online and he learns from his elder brother, friends and websites. He does not tell his parents what he is doing on the Internet and his parents, too, according to him, are not interested in finding out what he is up to.

He holds the view that children and youth should use the Internet to be successful in life. He says that he feels miserable when he can't access the Internet for a few days. Checking his Ordinary level examination results had been the most memorable experience of his online life. He is also very happy that he found his girlfriend through the Internet.

Table 27: The most memorable, positive experiences of online-IT users, percentage

Memorable experience	 (2,559)	 (1,878 users)	 (681 users)
Checking exam results	56.4%	57.4%	53.7%
Reading e-books	28.2%	26.8%	32.1%
Uploading own creations	22.5%	26.4%	12.0%
Submitting an article/report	14.8%	14.2%	16.4%
Identifying a university/school	12.2%	13.2%	9.5%
Securing a scholarship	2.7%	3.3%	1.2%
Doing an online exam	3.5%	4.2%	1.8%
Taking an online class/course	5.5%	6.1%	4.0%
Finding a boyfriend	-	-	2.8%
Finding a girlfriend	-	10.9%	-
Receiving/giving a gift	2.9%	3.0%	2.5%
Planning cost-effective trips	10.0%	10.6%	8.2%
Purchasing products	12.8%	15.2%	7.2%
Selling products	4.2%	5.5%	0.7%
Making an important payment	2.7%	3.1%	1.8%
E-channeling a doctor	5.1%	5.5%	3.8%
Obtaining advice	12.7%	14.9%	6.6%
No memorable experience	17.2%	14.7%	24.0%

Analysis based on multiple responses

4.13 IT teachers in government schools

Of the 77 government-school IT teachers surveyed in this study, most were women (66.7 per cent), and 84 per cent held an IT degree or IT diploma. According to the school survey, which covered 61 schools, about 15 per cent of the schools, especially the rural schools, had no online connectivity in their computer labs. Nearly all the IT teachers stated that their training on educating children on online security and safety issues was insufficient. They had not received any specific training on how to safeguard children who encountered online security and safety problems.

The IT teachers noted that the schools did not have a commonly accepted policy on allowing children to access the Internet. For example, in some schools, 11-year old children were admitted to the IT lab, but in most schools the age limit was 14 years old. The major purpose for allowing children to access Internet in the IT labs was to enable them to search for educational information. However, over 66 per cent of the teachers reported that children used the IT labs to access social media.

Of the 77 IT teachers surveyed, only 40 responded to the specific question on incidents of abuse and threats experienced by children; however most of them were aware of incidents of abuse and threats experienced by students. The teachers' observations give a general sense of the types of abuses that occur though the Internet in school settings:

- Receiving messages stating that they had won prizes
- Posting or forwarding photos of someone to make that person feel embarrassed
- Hacking passwords and information
- Spreading incorrect information/malicious information about a person

4.14 The knowledge gap between online-IT users and duty bearers/key stakeholders

Discussions with parents revealed that they were unaware of the pros and cons of children's Internet usage. Key informants interviewed for this study said that most parents had a negative attitude towards technology and were suspicious of social media. It is also apparent that there is a gap in knowledge of IT-related topics between adults and children, which can lead to a lack of appropriate parental supervision and a lack of parental ability to educate children on online safety.

“At focus group discussions, parents said

...as we don't know how to operate these devices, we cannot monitor what our children are doing.”

“We think children should concentrate on homework and that they should not be allowed to use smart phones and computers....”

“Children nowadays are smarter than we are and they know how to use technical gadgets.”

“We have no time to supervise all the engagements of children. We go to work in the morning and come back in the evening....”

“We have heard, through mass media, that many bad things are happening to children who are online...”

”

Children grow up with exposure to TV, telephones, mobile phones, the Internet and social media. As a result, they have acquired advanced computer skills and use these devices and according to the key informant interviews, children mostly demonstrate good judgment at searching, processing and synthesizing information that is needed for their school projects. Children are also more participatory in their online world, and freely shared information and knowledge they deemed important, with their peers.

Children who were non-Internet users are often a reflection of an adult's negative attitude towards technology. As many as 41.8 per cent of children said they did not access the Internet as their “parents did not allow [them] to use the Internet”. In contrast, 16.5 per cent of the online-IT users said their parents had taught them how to access the Internet and parents paid their mobile phone and Internet bills. According to the key informants, the level of education, professional and social status of the parents influenced their perception of the Internet, and consequently, how they advised their children to access the Internet.

Box: 4

Trends in children's online-IT behaviour

The IT knowledge of the current generation is higher than that of the previous generations. The new generation's exposure to TV, telephone and the mobile phone from the early stages of their lives have influenced them to increase IT knowledge.

“The interaction between adults and kids around these technologies has improved a lot”

Children know how to operate a mobile phone quite well (without training) even better than their elders and they know more words too. ICT (apps) can be helpful in improving English language pronunciation even in the early childhood stages.

Mr. A. A. S. Atukorala
Deputy Director, Children's Secretariat

Today, the primary method of accessing the Internet is via a mobile phone or another mobile device, not a PC. Awareness about what these devices can do is very limited among the guardians (when they buy/provide these devices to children). It is difficult for guardians to track online activities of children.

“Age of the first interaction (with the Internet) with the web has come drastically down”

Their first entry point devices are iPad type ones, not PCs. Parental protections on these digital devices are very basic (compared to PC versions). Android and iOS increased the capacity for parental control recently. Security on Android is very poor in particular. In online purchasing and app downloads, parents find it difficult to control children who are online. These issues are not sufficiently taken up by media.

Mr. Sanjana Hattotuwa
*Senior Researcher,
Centre for Policy Alternatives*

Providing sex-education to children will be useful. Such education should be about biology and the interpersonal aspects of sex to provide children with a broader perspective. When the children understand these subjects they wouldn't go to experiment, instead they will be able to control their sentiments and make appropriate judgements.

“Tight parental control of children's social interactions, pushes children to go online”

Tight parental control of children's social interactions, pushes children to go online and explore social relations over social media. Educate principals/teachers/children about the Internet (e.g. in some schools students are not allowed to open a Facebook account).

Mr. Dumindra Rathnayake
Former CEO, Etisalat Sri Lanka

Policies are not based on current realities, so people don't understand what some concepts or words (e.g. rights) mean. NCPA is partly involved in online security but this requires further improvement and active engagement. The real experts are the kids and we have to learn from them. But our policymakers are not ready to take to this bottom up approach. Teenage affairs are often criminalised and they end up with the police and in court. Youth are constantly in battle with society.

“Within the mandate of child protection, online-security is a small subject area”

And the NCPA's capacity is limited. The penal code's definitions may be somewhat applicable to address online security, but definitions of, for instance, 'evidence' (e.g. defining email, social media sharing) need to be improved. SL CERT and ICTA have been working on this together with the NCPA.

Mr. Sajeewa Samaranayake
Deputy Chairperson, NCPA

5. ONLINE SAFETY OF CHILDREN IN SRI LANKA

5.1 Introduction

Having a profile on social media has become an important part of many children's online lives. Many children want to engage in discussions with friends, send messages and listen to music when they are at home. Depending on the digital device that children use, the sites they access on the Internet are often unknown to their parents or teachers. Therefore when something detrimental happens, the parents or teachers may be unable to intervene.

During key informant interviews, almost all the subject experts in the country (from government and NGO to academia) recognized that online security and safety of children in Sri Lanka was an issue of increasing concern. Organizations such as Sri Lanka CERT, confirmed that the number of complaints related to online security was on the rise.

Box: 5

Cyber security and child protection in Sri Lanka

According to SL-CERT, a total of 2,967 cyber security incidents, including child-related issues, were reported in 2015; 96 per cent of these related to social media. The number of social-media-related incidents that have been reported has increased each year, beginning with 49 incidents in 2008 to 2,967 incidents in 2015.

'Child Line: 1929', the hotline maintained by the NCPA has received over 61,000 calls reporting all types of child abuse and seeking counseling, as reported in Ceylon Today on 2 January 2014.

In 2015, according to communications to the research team from the NCPA, 10,732 cases were reported to the NCPA and most of them were from the Western Province.

“ Children will access free wifi (at wifi hotspots) even if their phones were controlled by parents, and did not have data access. Children are smarter than parents, especially with iPads and smart devices. The only way to prevent abuse is through educating children ”

Mr. Dumindra Rathnayake
Former CEO, Etisalat Sri Lanka

“ Some parents tend to use technology as a tool to keep the children occupied with digital gadgets and to keep them entertained. By doing so, such parents avoid their parental responsibilities. This behaviour leads to attitudinal damage of children (emotional insecurity, etc.) and leads them to experiment with unsafe aspects of the Internet: it can also potentially lead to addiction to the Internet ”

Mr. Charitha Ratwatte
Head Digital Inclusion and Sustainability of Dialog

¹²Communication to the research team by the principal information security engineer, SL-CERT, January 2016

“ In recent years, there have been public debates even at parliamentary level about the appropriateness of social media for children. As the children’s age of first interaction with the Internet is drastically coming down, relevant authorities and guardians question the appropriateness of introducing computers to children at an early age (e.g. 3-5 years). Therefore the chairperson suggests that in the early stages, age does not matter. Even a five-year old should be allowed to access the Internet, but access should be controlled by parents ”

Mr. Roshan Chandragupta
Information Security Engineer, SL CERT

This chapter aims to provide a detailed analysis of the current status of online safety of children. As the first step, a systematic effort was made to understand the international perspectives on the subject of online security and safety. Thereafter, the insights gathered from the survey are assessed against the international framework, to provide a clear, in-depth perspective of the current status of children who are online in Sri Lanka.

5.2 Threats: the global perspective

In the evolving subject of ‘online security and safety’, following is a selected list of threats that are frequently highlighted in the global body of literature:

Safety and security of personal computers Exposure to computer viruses is a common threat as many users often fail to install appropriate firewalls and antivirus software. This is a threat to the hardware, but the danger is the loss of information. This threat is not discussed in this analysis.

Online identity theft (Get Safe Online, 2015) is stealing someone’s identity information such as name, date of birth or passport information, to execute fraudulent activities by impersonating that individual on the Internet. Such activities may involve unauthorized financial transactions or obtaining credit cards. These threats result in loss of money.

Compulsive / Addictive use of the Internet (Davidow 2012, Srinivasan 2014) is defined as compulsive, pleasure-seeking behaviour where a person becomes obsessed with Internet applications and activities such as blogging, playing online games, social networking and online gambling. Internet addiction is often associated with gaming, gambling and pornography. Compulsive use of the Internet often leads (Mitchell et al 2005) to unauthorized use of parent’s email addresses and credit cards by children to access online material.

Spamming is also known as junk mail, which is sent through unsolicited emails to a recipient in bulk, often with vested interests. This is not seen as a risk to children, except of it being a waste of time and as an activity that slows down Internet access.

Phishing (Insafe 2015) happens when people respond to fake emails, which usually appear to come from a reputable source such as a bank, asking the recipient to enter personal information such as bank account details, which is then misused.

Infringement of copyright occurs when online users share and exchange files such as music, films, videos and games, with other users without respecting the copyrights protected by law. This is a crime under national and international conventions.

Unwanted advertising is a regular activity where some companies target children to market their products and use online services to sell their products to children. They acquire user information and disseminate material without the consent of the user.

Sexting (Childline UK 2015) is another phenomenon where children put themselves at risk by posting sexually provocative images of themselves online or by sending them to friends using mobile technologies such as text messages.

Grooming is the abusive use of the Internet and mobile phones by adults to make contact with children for sexual purposes. Grooming more often takes place through a process which begins by acquiring personal information through social networking spaces, and then by systematically gaining the confidence of the children for sexual exploitation.

Cyberbullying is threatening behavior such as sending threatening text messages, posting unpleasant things about people and circulating unpleasant pictures or videos of someone. The degree of risk posed by these online threats is different and complex, as explained in the following section.

5.3 Risk vs harm: The global perspective

The global research literature (including from developing countries), emphasizes that the relationship between risk, harm and safety of children in online settings is enormously complex. It is necessary to understand that the exposure to risk does not equate to actual harm (Livingston and O'Neill, 2014). For example, things like phishing, spamming and unwanted advertising, are forms of risks, whereas cyber bullying and grooming can cause direct harm to a child. The global research (Third et al, 2014) explains that the children are knowledgeable about the range of risks, such as 'seeing things they did not want to see' (e.g. violent content) online. Similarly, the literature noted that children acknowledged the need to keep their information safe and the potential problems associated with their 'digital footprints'. Some children had even recognised that participation in digital media may be a risk to their physical health and well-being.

Furthermore, the literature emphasizes that harmful aspects, such as cyber bullying, do not preoccupy children to the same extent that it often features in public and policy debates. Cyber bullying, contact with strangers, sexting and pornography are found to affect nearly 20 per cent of adolescents. Most children recognise these threats as a challenge to their right to be safe. (Livingston and O'Neill, 2014)

Some children are more vulnerable to harm as a consequence of exposure to online risks than others. National resources and policy efforts should be focused more precisely to target such children and to prevent them from being harmed.

Children have a right to access the Internet for information and civil participation, and attempts to protect children that impeded their access violates their child rights. Children learn and develop resilience when they educated on risks and how to safely respond to risk.

5.4 Risks to online-IT users



The previous chapter showed that a considerable number of boys, and nearly 10 per cent of girls, have reported having a relationship with people they met online. These children's safety and well-being may be at risk depending on who these people are. It is important to note that the study did not inquire about the age of the people children had met online.

Around 15.1 per cent of children with access to the Internet had divulged their personal information to others online (both persons and websites). While only 1.9 per cent of girls had divulged their personal information, an alarmingly high 19.7 per cent of boys had done so. Sharing personal information and pursuing these online relationships could have exposed this group of children to online security threats.

Another 21.5 per cent of children with access to the Internet had taken a chance and had continued to provide personal information to strangers; however, they had done so using fake identities. This group was composed of 23.5 per cent boys and 15.7 per cent girls. Although it seems this user group had taken a step to ensure their security, by continuing their association with online - strangers, they too remained vulnerable.



On the positive side, 63.4 per cent of children, of whom 82.4 per cent were girls and 56.8 per cent were boys, had ignored requests for personal information by strangers, and had reportedly abandoned the website where the request happened. The percentage of this prudent group of online-IT users (around 60 per cent) did not vary significantly among the different school grades (6 - 9, Ordinary Level and Advanced Level), and the different ethnic groups (Sinhalese, Tamil and Muslim).

Table 28: Children’s response (as percentage of sampled population) to online strangers’ requests for personal information: by gender, ethnicity and grade

Response to requests for information by children	Gender		Ethnicity			Grade		
			Sinhalese	Tamil	Muslim	Grades 6-9	Ordinary Level	Advanced Level
Gave true personal information (name, age, e-mail address & phone number)	19.7%	1.9%	12.9%	18.4%	22.6%	16.0%	12.6%	17.3%
Gave fake name, age, e-mail address & phone number	23.5%	15.7%	23.2%	15.8%	23.1%	20.5%	26.1%	23.1%
Ignored the request/ abandoned the site	56.8%	82.4%	63.9%	65.8%	54.3%	63.5%	61.3%	59.6%
Total	1518	529	1396	380	234	658	923	979



Children’s response to the question, “Have you physically met any persons you had previously met online?” provides further insights into the risks. Around 27.9 per cent of children online had physically met people that they had first met online. Another 25.2 per cent of online-IT users anticipated meeting in person in the future. Once again, this user group was composed of more boys than girls. Although the study did not probe deeper into the ages of those individuals that the children had met up with, most of those who reported having met someone indicated that these people fell into the category of someone they had befriended, or someone related to a job offer or social activity, like a club or organization, rather than as a person for a prospective romantic relationship.

Table 29: Response to the query on physically meeting people, previously met online, as a percentage of sampled population, by gender

Response	Total %		
No, I have never met anyone.....	46.9	41.4%	67.7%
Not met yet, but I would like to meet such a person in the future.....	25.2	28.7%	11.9%
Yes, I have met.....	27.9	29.9%	20.4%

Of the children who had physically met online-strangers, 18.3 per cent (boys and girls) had done so without informing anyone, and another 36.3 per cent had only informed a friend, underscoring the degree of risk these user children were being exposed to.

Table 30: Action taken during offline meetings with strangers befriended online, percentage of sampled population by gender

Action Taken	Total		
Did not tell anyone.....	18.3%	18.2%	19.2%
Told a friend.....	36.3%	38.1%	24.0%
Told a family member.....	32.4%	33.0%	28.0%
Other*.....	13.0%	10.7%	28.8%
Total.....	100%	100%	100%

*Note: Meeting under different circumstances, such as the stranger coming to see the children or the children meeting them accompanied by relatives and friends, indicating that the meeting was not alone.

Analysis based on multiple responses

A substantial proportion of children with Internet access are engaged in risky behavior. Most social media platforms offer users the option to manage their privacy settings, giving the users more control over who sees their information. It is important to note that on many sites, the default privacy setting is low and a person's information is available to most other users. Nearly one in four boys and one in three girls were not at all aware of 'privacy settings' for their online accounts. Around eight per cent did not know how to change privacy settings. However, there was another group of online-users, 32.2 per cent of boys, and 33.1 per cent of girls, who were aware of privacy settings, but did not want to set them up. All these children are exposed to potential online threats.

Table 31: Action taken by children online to change the privacy settings of their online accounts: by gender, grade, sector and ethnic origin



Action taken to change privacy settings			Grades 6 - 9	Ordinary Level	Advanced Level
I am not aware of privacy settings	24.5%	29.2%	43.3%	23.6%	17.1%
I do not want to set up privacy settings	32.2%	33.1%	29.4%	33.0%	33.4%
I do not know how to change privacy settings	7.6%	8.5%	8.1%	9.7%	5.9%
Yes, I have changed my privacy settings	35.7%	29.2%	19.2%	33.7%	43.6%
Total	1,517	353	432	661	778

Table 31: *Contd.*

Action taken to change privacy settings	Urban	Rural	Plantation	Sinhalese	Tamil	Muslim
I am not aware of privacy settings	16.6%	31.4%	30.5%	25.1%	24.2%	28.9%
I do not want to set up privacy settings	35.0%	31.1%	19.4%	33.5%	30.8%	28.1%
I do not know how to change privacy settings	7.0%	8.1%	11.1%	7.9%	8.8%	6.3%
Yes, I have changed my privacy settings	41.4%	29.3%	39.0%	33.5%	36.2%	36.7%
Total	758	1,060	36	1,247	364	256



5.5 Indicators of exposure to risk

In order to improve clarity, indicators were developed in this study to analyze online behaviour by following the international guidelines developed by International Telecommunication Union (ITU) (2009). From the global perspective of online-IT security of children, ITU's guidelines on online security highlight the following five areas where children are exposed to risks and are vulnerable, which can be seen as indicators of risk:

1. Content: information that the users access or upload
2. Contacts: known and unknown 'friends', children interact with on the Internet
3. Conduct: how the users carry out online activities respecting ethical, legal and other responsibilities
4. Commerce: how the users' online activities may lead to inappropriate commercial transactions
5. Excessive use: obsessive or compulsive engagement with the Internet

Considering these indicators, children in Sri Lanka are clearly exposed to some risks.

Table 32: Indicators of exposure to risk: as a percentage of sampled population by gender

Improper behavior	Total (2,560)	 (1,879)	 (681)
Content: Sent/uploaded texts, images, videos, photos more suitable for adults	10.7%	11.9%	7.3%
Conduct (any of the following four actions):	24.7%		
Lied about their age	13.1%	14.4%	9.3%
Engaged on social media with false information	16.7%	18.6%	11.6%
Used others' passwords to log into their profiles	5.1%	5.7%	3.5%
Sent messages that could be nasty or could hurt someone's feelings	24.8%	27.4%	17.6%
Contact (any of the following three actions):	41.3%		
Accepted chat requests from strangers	21.9%	24.6%	14.4%
Shared photo with a stranger	14.3%	17.2%	6.3%
Shared personal information with a stranger	8.0%	9.3%	4.5%
Commerce: Engaged in inappropriate online shopping	30.9%	35.4%	18.5%
Excessive use: Using the Internet several times a day	28.7%	34.0%	13.7%

Some explanatory notes on these indicators are provided below.

A. Inappropriate Content

One in ten children (a considerably higher percentage of boys) admitted that they had sent/uploaded content inappropriate for their age, which included photos and videos. The proportion of such children increased slightly from Grades 6 - 9 to the advanced level, but the percentage of girls remained low throughout (about three per cent). A much higher percentage of Muslim (16.2 per cent) and Tamil (15.4 per cent) children, almost double that of the Sinhalese children (8.6 per cent) were accessing content that could put them at risk.

Table 33: Percentage of children who shared inappropriate content online

Gender Breakdown by Grade

Grades 6 - 9 (8.7%)		Ordinary Level (9.1%)		Advanced Level (10.6%)	
Boys (10.3%)	Girls (3.2%)	Boys (11.5%)	Girls (2.5%)	Boys (13.7%)	Girls (2.8%)

Gender Breakdown by Ethnicity

Muslim (16.2%)		Sinhalese (8.6%)		Tamil (15.4%)	
Boys (18.5%)	Girls (10.0%)	Boys (9.4%)	Girls (6.1%)	Boys (17.7%)	Girls (10.0%)

B. Contacts with Strangers

Four out of ten online-IT users admitted sharing photos (including personal photos), and personal information with persons they hadn't known before, and had even accepted chat requests from strangers. Though this study did not look into the type of strangers that children interacted with, or the nature of their interactions, these types of behaviour can expose children to sexual predators or harmful online communities.

These interactions captured above could have been between children or adults, but this was not verified in this research. Furthermore, children admitted to sharing their own photos with strangers. These findings are in line with the harmful and often illegal online activities described in the ITU guidelines.

Box: 5

National media and online security in Sri Lanka

Both print and electronic media in Sri Lanka have taken a special interest in online security in recent years, which escalated in 2014. Among the highlights were the three incidents of girls aged 14, 16 and 19 years old, reported in Movement Against Bullying (2015), Lanka Newspapers.com on 23 August 2010, and News1st on 19 February 2014 committing suicide as a result of social disputes that were directly linked to Facebook, according to the police media spokesperson. Such incidents brought social media, Facebook in particular, into the center of a major public debate. This debate has contributed to controversial comments and discussions at the parliamentary level, as reported in Republic Square on 10 October 2013 where the possibility of banning Facebook and regulating (Freedom House, 2014) social media in Sri Lanka was discussed in 2013 and 2014.

According to reports from Sri Lanka CERT, there were 2,976 cyber-security related incidents reported in 2015, and 96 per cent of them were linked to social media. The number of such social-media-related incidents has increased each year, beginning at 49 incidents in 2008 and rising to 2,850 incidents in 2015. The 'Child Line: 1929', the hotline maintained by the NCPA, has received over 61,000 calls reporting child abuse and seeking counselling support.

Most of the cyber bullying victims in Sri Lanka are girls aged 13 to 18 years, according to the online campaign site, 'NoBullying.com'. Cyber bullying incidents reported in Sri Lanka are often 'relationship bullying', such as boys bullying girls as revenge for ending their relationships. For example, a boy posts or shares a nude photograph of his ex-girlfriend on a social media network, as evidenced by several articles in Lankadeepa newspaper in November 2014, or worse, uses editing tools to create pornographic images of the ex-girlfriend, as reported in the same newspaper in 2014 and 2015. There were also incidents of boys using fake social media profiles to gain trust and acquire confidential information to subsequently bully the victim.

In addition to cyber bullying, there were other incidents reported in Lankadeepa newspaper, including online lottery scams, phishing and mobile SMS-based sexual harassment.

C. Inappropriate Conduct

Nearly a quarter of online-IT users admitted to inappropriate conduct such as lying, sharing false information, sending messages that could hurt someone else, or admitted to using others' passwords to log into their accounts. Such activities constituted unethical and unlawful behaviour.

D. Commerce

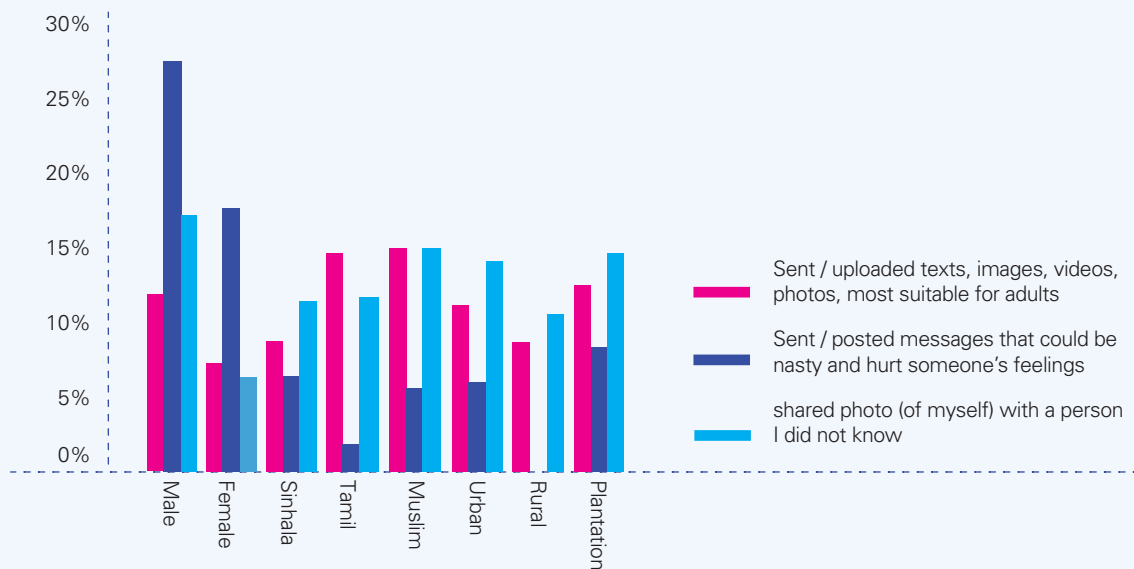
Nearly one in three children engaged in some form of commercial activity online. Some children searched for jobs and products to explore designs, prices, etc. In addition, children admitted that they had lied about their age and that they had engaged in social media with false information. As explained in the ITU guidelines, such inappropriate online behaviour can potentially lead to commercial exploitation, and privacy and data protection risks.

E. Excessive use

Of children who took the survey, 28.7 per cent accessed the Internet more than once per day. Parents, teachers and key informants expressed concern about excessive use of the Internet by children. However, it is not clear from the results of this study whether excessive use was negative. For example, whether there was a negative impact when children got used to accessing the Internet for educational purposes (as noted above) and when the need to access the Internet increased with the need for more information.

Through these indicators, it is clear that some of the globally known online security threats are visible among the children who are online in Sri Lanka. There is indirect evidence to suggest that children are exposed, knowingly or unknowingly to acts of infringement of copyright laws, online identity theft and cyber bullying. Given children's very low interaction with email, no evidence was found of them engaging in spamming and phishing. There was also no direct evidence of grooming.

Figure 15: Children engaged in risky behavior: as a percentage of sampled population



5.6 Reporting process for online abuse

Children were very poorly informed about which authorities they should approach in the event of being a victim of online abuse, with 83.7 per cent indicating they were unaware of where to report online issues. Only 16.3 per cent of children in the study said they knew whom they should report to in the event of online abuse. When they were asked to name the responsible authorities/organizations they could report to, only 2.6 per cent of the children were able to do so. This indicates a clear gap in children’s awareness of methods of handling online issues when they arise.

Parents and children are also unlikely to report online security incidents to the police, as the victimized child might be subject to undue probing by the police. Very often, the child and his/her parents, have to engage in lengthy legal battles when they report security issues to the police. For serious cases of online abuse, there needs to be a child-friendly and rights-oriented process for reporting and seeking recourse with the authorities. However, for cases that do not warrant police intervention, there is a clear need for education of children and parents around prevention and monitoring of online security and abuse, complemented by robust community-based recourse mechanisms that are easy for parents and children to access.



Table 34: Children’s knowledge on where to report online abuse

Institution or person to report online abuse to	Number of children (2,560)	%
Report to NCPA/ Call 1929	13	0.5
Report to police	35	1.4
Report to Facebook authority	14	0.5
Report to UNICEF	4	0.1
Subtotal	66	
Tell parents, teachers and friends	352	13.7
Subtotal	418	
Not aware	2,142	83.7
Total	2,560	100

5.7 Learning about online safety

Children did not have a clear idea of the sources for reliable information on online security. Neither teachers nor parents had sufficient knowledge on the subject of online security. In this context, the majority of children depended on their siblings (34.7 per cent) and friends (41 per cent) to learn about online security. Furthermore, according to the expert opinions expressed during the key informant interviews, none of the institutions currently involved in children's online security in Sri Lanka has the capacity to design a programme that could be systematically introduced across the country to fill this gap.



Table 35: Children's sources for learning how to protect personal information and privacy online as a percentage of sampled population

Source	Total (2,560)	 (1,879)	 (681)
Not aware of any source	10.5%	11.3%	8.5%
From school teachers and ICT centres	11.5%	6.7%	25.0%
From parents	23.6%	18.4%	38.0%
From siblings	34.7%	31.5%	43.6%
From friends	41.0%	46.4%	26.1%
From mass media (TV, radio, newspapers)	24.0%	24.9%	21.4%
From websites	18.0%	21.2%	9.1%

Analysis based on multiple responses

Researchers also asked children about the people or institutions that they would like to learn about online safety from. Respondents definitively pointed to friends, IT teachers and siblings, reflecting their current sources of information on online safety.

Table 36: Children's preferred sources for learning about protecting personal information and privacy online: as a percentage of sampled population

Source	Total (2,560)	 (1,879)	 (681)
I do not want to protect my privacy or my personal information	5.7%	6.9%	2.5%
From school teachers and ICT centres	35.0%	35.1%	34.7%
From parents	27.7%	22.1%	43.2%
From siblings	30.9%	27.1%	41.3%
From friends	37.7%	42.0%	26.0%
From mass media (TV, radio, newspapers)	23.7%	24.3%	22.0%
From websites	21.1%	25.2%	9.8%

Analysis based on multiple responses

5.8 Policy Issues on Online Safety

According to the Commonwealth Telecommunications Organization, for many countries, especially in the developing world, clear national policies are not in place for the protection of children online. Sri Lanka currently does not have a clear national policy on online safety although the existing 'Computer Crimes Act' appears to cover many online safety issues (e.g. unauthorized access to computers could be considered a crime). The penal code's definitions of 'evidence' (e.g. definition of email, definition of social media sharing) seem inadequate to respond to the changing online reality for citizens. National experts consulted during this study agreed that the concepts, policies and operational strategies for the online security of children are still under debate.

Experts interviewed for this report agree that policies are not grounded in current realities, and therefore people do not understand what concepts and words such as 'rights' mean in general. Respondents said that the real experts are children, and it is important to learn from them. They also note the lack of penal code definitions that apply to online issues and a need to improve the definition of "evidence". At national level, the 'Computer Crimes Act No., 24 of 2007' can be used to prosecute against cybercrimes (obscene publications, sexual harassment and extortion). Proposals are being formulated by the relevant authorities to either strengthen or else to formulate a new act. The bill being formulated is titled the Act to Prohibit and Prevent the Publication, Distribution, Sale, Import and Export of any Matter, Object or Thing, which is Obscene'. This Act will repeal the Obscene Publications Ordinance (Chapter 30), and will provide for issues connected with a broader spectrum as the Act's title indicates.

In 2015, Sri Lanka signed the 'Budapest Convention on Cybercrime' the first international treaty that addresses Internet and cybercrimes, which has been very helpful to new efforts on national policy formulation. Policy guidelines prepared by the ITU at the international level could also be useful for designing national policies.

The NCPA, along with other government agencies, such as the ICTA and Sri Lanka CERT, have already begun initiatives to improve the foundations in terms of 'policy definitions' and institutional capacity to implement them. Proposals are being formulated and action is already underway by the NCPA to strengthen the existing legislative acts and formulate new legislation. For instance, a bill is being drafted titled: "Act to Prohibit, and Prevent the Publication, Distribution, Sale, Import and Export of any Matter, Object or thing which is Obscene; to repeal the Obscene Publications Ordinance (Chapter 30): and to provide for matters connected therewith or incidental thereto". The Children's Secretariat is currently reviewing the existing 'Early Childhood Care and Development National Policy' and is trying to ascertain the area under which ICT could be included in a revised policy on childhood care and development.

5.9 The role of institutions and their capacity

Legislative changes are an important basis for ensuring children's online safety; however there needs to be a broader infrastructure to address this issue. The National Child Protection Agency (NCPA) has the mandate to oversee this, however, the NCPA is experiencing serious capacity limitations in handling children's online security due to financial deficiencies and emphasis on other child protection concerns. First, the subject of online security is only a small portion of the child protection work that the NCPA is mandated to handle. Child protection from physical and sexual abuse has become a major issue due to often imbalanced media coverage. Under such a socio-political environment, donors and government organizations do not prioritize their funding for online protection.

Second, the Institution is short of senior-level staff leading to a lack of capacity to implement a broader agenda on online security issues. Experts interviewed for this report note that online security occupies a small area within the realm of child protection and is about 30 percent of the NCPA's overall work. The NCPA's current response to online security has been in a reactive 'fire-fighting' mode. Nevertheless, the NCPA has made an effort to appoint a task force with the mandate to investigate, prosecute and recommend required legislation.

Experts interviewed for this report note that when an incident is reported to the NCPA on the '1929 hotline' the follow-up process begins. The NCPA refers it to the police or the NCPA special police unit (which is staffed by 30 officers), and the CID's special cyber-crime unit for investigation. Organizing the follow-up process is difficult and the NCPA has to rely on the cooperation of other organizations. The NCPA's cadre of 120 is not sufficient to handle investigations effectively.

Key informants also note that Internet service providers have an important role to play in promoting responsible usage of social media.

Other institutions such as the Ministry of Education and the Police Department do not have sufficient staff capacity or budget allocations to handle children's online security issues. Institutions such as the ICTA, the Ministry of Telecommunication and Mass Media, the Ministry of Justice and private institutions such as telecom service providers, all recognize the importance of the issue, and carry out a few activities, mainly for raising awareness, about children's online security.

It should be noted that interventions to establish online security of children involve multiple fronts. Many national experts suggest adopting multi-stakeholder approaches that can engage schools, parents, youth clubs, regulatory bodies such as the NCPA, the police, religious centres and technology service providers.

5.10 Appropriate age of access

Institutions have varying policies on the minimum age for computer or Internet usage by children accessing their services. There are preschools and primary schools (both national and international) in Sri Lanka that allow Internet use by children, with varying limitations such as only for educational games or for other educational purposes. This type of access appears to be a trend in early learning and one which is attractive to parents in choosing early learning options for their children. Given that institutional access to computers and the Internet appears to be earlier in children's educational career, key informants in this study suggest a number of guidelines for children's early access.

1. Online access in early childhood should be carefully monitored and should take place under the careful guidance of adults.
2. Some experts argue that online access in early childhood should not be restricted at all. Every key informant agreed that controlling children's online access was not the right approach to online security. In an increasingly online world, restricting access may not bring positive results. Instead, a dialogue should be promoted around online security and the safe use of ICT, between parents, teachers and young children. They proposed that appropriate education and awareness should be the primary ways to establish online security, suggesting:
 - a. Education programmes targeting school principals, teachers, parents as well as children on online safety.

Programmes to educate children on the broader parameters of online safety (how to use a password and on careful handling of personal information such as names and dates of birth).
 - b. Programmes to educate duty bearers on how to skillfully handle children's online safety issues. This should include the provision of professional training (involving professionals such as psychologists etc.) for principals, teachers and student counselors.

5.11 Parental control of Internet use

Key informants note that denying children access to the Internet is not an effective tool to secure children online. It is important for parents to educate themselves and their children on prevention and reporting of online abuse. The parental control settings in mobile devices such as smart phones and tablets (especially, Android devices) are not as effective as they are on personal computers and easier to bypass, so require monitoring. Children use these mobile devices more often than computers to access the Internet. Furthermore, it is obvious from this research study that parents typically have a lower exposure and knowledge of IT than their children, which makes parental controls less effective, and parents' increased knowledge would make them more effective duty-bearers for keeping children safe online.

6. RECOMMENDATIONS

Based on this research, this study makes the following recommendations. These recommendations for the protection of children who are online, were formulated after a careful study of the international guidelines provided by the ITU for policy makers (2009). Additionally, these guidelines have been revised based on the opinions of a diverse set of national experts and on the findings from the school survey, focus group discussions with children and parents, and key informant interviews with IT teachers. This report's recommendations for the online safety of children are centered on 'empowerment' rather than 'control' of children.

A. Policies, laws and regulations

- i. Sri Lanka does not have a national policy framework on online access and online security. A policy framework is currently being developed by the relevant authorities and the concerned agencies should provide the necessary assistance for developing this policy framework. From a child rights perspective, this exercise should be participatory and include children themselves in addition to the government, academia, NGOs and private sector organizations. The private sector plays a vital role in ICT. Therefore, its involvement, specifically in the safe use of the Internet by children, is essential.
- ii. Based on the final policy framework, legislation should be enacted to ensure the safe use of the Internet by children. The 'Computer Crimes Act' should be revised with appropriate penal code definitions. The legal framework should cover (a) every crime that can be committed against a child in the real world (because such crimes can also be committed on the Internet); (b) Internet specific crimes such as 'grooming'; (c) misuse of computers for criminal purposes; (d) hacking of computers and other non-consensual uses; and (e) the behavior of children who misuse the Internet to abuse and bully their peers.
- iii. As a prelude to developing appropriate laws, a comprehensive review of the current regulations, especially their weak areas on combating cybercrime, abuse and related aspects, should be undertaken. This review should also evaluate the capacity of the regulatory authorities to effectively implement their mandate. The review team should be appropriately set up to include expertise in all relevant subject areas.
- iv. A self-regulatory body of industry (telecom and IT in particular) partners should be established to develop and publish 'codes of good practices' to guide the Internet industry on measures required to keep children safe online. Such a body should publish codes applicable to social networking sites and mobile phone networks regarding their content and services offered to children. The 'Guidelines for Industry on Child Online Protection', published by ITU and UNICEF (2014 Edition), should be followed in formulating child online protection policies that focus on the industry.
- v. The mechanism for reporting cyber security related incidents should be improved. The current national hotlines managed by the NCPA and Sri Lanka CERT to service different aspects of online security should be improved and their capacities expanded to enable them to handle a higher volume of calls on a 24/7 basis. Furthermore, it is necessary to improve the organizations' monitoring, evaluation and feedback mechanisms to enhance the impact of the hotlines.

The NCPA and SL CERT should collaborate with international organizations such as the Internet Watch Foundation to improve their ability to effectively control online abuse, for example, by using digital fingerprints to remove abusive images.

B. Advocacy and capacity building

- vi. The Ministry of Education should lead on developing educational and training material targeting children, parents, teachers, duty bearers and the general public, for awareness campaigns on online safety. Using these materials, the relevant regulatory authorities should conduct Training of Trainers (TOT) courses for selected groups from related organizations and enlist them to conduct awareness programmes.

The relevant authorities should compile a sourcebook which serves as a practical guide on online safety. A large amount of educational material on children's online safety is already available online and in national organizations, including corporate organizations. However, there is a need to adapt these materials to suit the local culture and for availability in the local languages.

In view of the generation gap on IT literacy, the educational material should be produced in easily understandable, jargon free language, in multiple media, audio, video and printed formats, and in all three languages, and aimed at adults as well as children.

National and regional campaigns should be organized to create awareness on online safety for children and to introduce the sourcebook and practical guide to the public. Such campaigns should aim to set the right tone, for instance, to overcome the fear of technology, and give due prominence to the new technology's role in offering children positive and fun features, and their capacity for creating empowerment opportunities for children for inclusivity and participation in society as responsible citizens.

- vii. Officials at all levels of the regulatory authorities should receive thorough short-term training on the use and misuse of the Internet. The trainings should include the legal landscape of children's online access.
- viii. Awareness programs should be organized for high ranking officials of regulatory bodies and politicians (national, provincial and local government) to persuade them to increase the budgetary allocations for online safety programmes. When there is public support from the government and politicians, it is likely that non-governmental organizations will come forward to support and fund online child protection activities.

A donor consultative meeting should be initiated to share expert opinions and findings of related studies on children and the Internet.

The media are a very effective medium for shaping national opinion. Therefore, a series of workshops on online safety should be organized at national level, targeting media personnel. Media personnel and media agencies should be encouraged to enlist the assistance of national experts in their media coverage of online safety issues. The NCPA and other regulatory bodies should provide the necessary information, personnel and materials, such as documentaries and brochures, to be used by media agencies in their programmes.

Research

- ix. There are significant research gaps in children's online protection identified through this study. There needs to be more timely and accurate national data on the excessive use of the Internet, the influence of cultural and generational gaps on online behaviour and the impact of participatory engagement and online security within the context of child rights. Support should be provided to undertake new research on the above topics with the objective of influencing policies, campaigns and capacity building programmes on online security of children to respect children's rights to participate.

Technology

- x. Introduce technological solutions such as apps, specialized mobile SIMs, and specialized mobile handsets, for young children, to enable their safe use of the Internet. The Information and Communication Technology Agency (ICTA) of Sri Lanka, as the leading ICT institution of the government, and corporate companies, especially telecom partners, can take the lead role in this activity. Within this context, wider recognition of already existing initiatives introduced by the state and private sector, particularly telecommunication service providers in Sri Lanka, is also recommended.
- xi. Internet service providers (ISPs) should be encouraged to introduce network-level parental controls to customers, which would give the parents the choice and the means of protecting their children online. Lessons can be learnt from the countries where such practices are in place (e.g. the United Kingdom).

Given the expansion of Wi-Fi hotspots in towns and cities in Sri Lanka, it is also recommended that the 'kitemark' is introduced to support the accreditation of child-friendly Wi-Fi zones.

- xii. Given the potential expansion of e-commerce and online payment methods among children, a rigorous age and identity verification processes should be set up as soon as possible to enable secure billing relationships between vendors and customers.

Use of networks

- xiii. Most schools have effective and active student societies and clubs that engage in a variety of child-centered development work. These societies should be encouraged to do awareness-raising activities to protect their online peer groups with the support of IT teachers, student counsellors and computer clubs and societies in schools. Schools should support these societies in obtaining financial support from school development societies, old boys'/girls' associations, the private sector and well-wishers, to implement programmes on child protection, which include online safety awareness.
- xiv. Although child protection societies have been established at district, divisional and grama niladhari levels, most are not functioning due to a lack of trained officials. Therefore, divisional level officers of relevant government agencies should be provided training on online safety, which in turn, will make grass-roots-level officials more effective. Divisional level societies could seek financial support from NGOs, INGOs and the private sector to implement such programmes.

Curriculum development and IT labs

- xv. The Ministry of Education should review the school curricula and incorporate age-specific lessons on online safety into the IT curriculum (or any other related subject) to build students' knowledge of digital literacy and safety on the Internet. Furthermore, the NCPA hotline telephone number (1929) should be prominently displayed in the relevant school text books and on school computers.
- xvi. Traditional values, norms and customs still play a significant role in influencing the behavior of adolescents and youth in Sri Lanka. Due to the influence of these traditional norms, sex education is not covered in detail. The Ministry of Education should review and revise the sexual and reproductive health education in the curriculum, to include online sexual exploitation. Meanwhile, as a short-term measure, school teachers should be trained to teach reproductive health to students using appropriate materials.

- xvii. Children showed a preference to learn online literacy from their school teachers. Therefore, IT teachers have to be trained and the Ministry of Education should ensure these teachers play an active and effective role. They should be given a thorough training on computer hardware and software, online security and be made aware of the organizations that can be contacted in the event of an online risk to a student.
- xviii. The Ministry of Education should promote the e-thaksalawa programme among school children (currently only 16 per cent access this website) and teachers. This website has almost all the required educational material, but even teachers are not using it. If teachers use this site to teach and give web-based assignments, students will use e-thaksalawa for educational purposes.
- xix. Given the popularity of social media among children, government authorities whose mandate is child welfare, should use social media as a channel to promote awareness about online security.

According to the findings of this study, children were unaware as to whom they should complain to regarding online abuse. The Ministry of Education and respective partners and caregivers need to make children aware of the different reporting mechanisms available to them. One specific recommendation is that the Ministry of Education should produce and distribute an attractive poster (a hard copy) with details of how and to whom children should complain. Information on hotlines should be included on this poster. This poster should be displayed on walls inside the IT labs accessed by children. It is the responsibility of respective stakeholders that these reporting mechanisms are sufficiently resourced to respond to and follow up on complaints made by children.

- xx. Preschool is a good place to start building children's Internet skills. It is assumed that when very young children are encouraged to use the Internet under the guidance of a trained preschool teacher, and when online literacy is built into their education. Each provincial council should carry out a pilot project by providing the necessary training, equipment and connectivity to a few preschools. The World Bank has earmarked funding for early childhood development and infrastructure for preschools for five years. Provincial Councils, together with the National Children's Secretariat, could commence a pilot project with these funds.

This study has made a significant contribution towards understanding the key characteristics of the digital landscape in relation to children in Sri Lanka. The report highlighted issues of children's access and use of the Internet, and identified knowledge gaps in children's use of the Internet and their online safety. The study also provided a series of recommendations, in particular, for duty bearers and policy makers. The recommendations proposed in this study focus on protecting children from online threats, while empowering them to use the Internet safely, to ensure children in Sri Lanka can be responsible digital citizens.

REFERENCE LIST

- 'Be cautious when using Facebook, Experts warn', *News1st*, 22 February 2014.
- 'Elpitiya girl commits suicide possibly over Facebook image', *News1st*, 19 February 2014.
- 'Evidence from Sri Lanka', *Lankadeepa online*, 7 September 2014.
- 'Evidence of phishing in Sri Lanka', *Lankadeepa online*, 12 December 2014.
- 'Evidence of using a fake profile in Sri Lanka', *Lankadeepa online*, 25 January 2015.
- 'Evidence on fake lottery scams in Sri Lanka', *Lankadeepa online*, 21 December 2014.
- 'Hitawathie.lk', 1 February, 2015,
Available from <http://www.hithawathi.lk/wp-content/uploads/Lankadeepa/Lankadeepa_art_7.jpg>
- 'Interview: What is Relationship Bullying?', *NoBullying.com*, 5 November 2014.
Available from <<http://nobullying.com/what-is-relationship-bullying>>
- 'NCPA hotline exceeds 61,000', *Ceylon Today*, 2 January 2014.
- 'News report from Lankadeepa (newspaper) online', *Lankadeepa online*, 11 November 2014.
- 'News report from Lankadeepa (newspaper) online', *Lankadeepa online*, 4 November 2014.
- 'President says Facebook is a "disease" in Sri Lanka', *The Republic Square*, 10 October 2013.
- Childline UK (2015). 'Sexting'. Available from www.childline.org.uk/Explore/OnlineSafety/Pages/Sexting.aspx.
- Davidow, Bill (2012), 'Exploiting the neuroscience of Internet addiction', *The Atlantic*, 18 July.
- eNovation4D Ltd (2015). Database of Top Sites Accessed in Sri Lanka.
Available from www.alexacom/topsites/countries/LK. Accessed 15 March 2015.
- 'Facebook love ends in suicide, Sri Lanka'. *Lanka Newspapers.com*, 23 August 2010.
- Freedom House (2014). 'Freedom on the Net.'
Available from <<https://freedomhouse.org/sites/default/files/resources/Sri%20Lanka.pdf>>
- Fusion Sarvodaya ICT4D Movement (2015). 'IT Yahamaga – Engaging Grassroots Youth in Using Technology Securely'.
Available from <http://fusion.lk/it-yahamaga-engaging-grassroots-youth-in-using-technology-securely>.
- Get Safe Online (2015). 'Get safe online free expert advice'.
Available from www.getsafeonline.org/protecting-yourself/safeguarding-identity.
- Insafe (2015). 'The digital universe of your children'. Available from
www.saferInternet.org/c/document_library/get_file?uuid=24d6a907-b16a-42b0-9bf9-c7d59c6375d3&groupId=10137.
- International Telecommunication Union (2009). Guidelines for policy makers on child online protection, ITU, Geneva, Switzerland
- International Telecommunication Union and UNICEF (2014). *Guidelines for industry on child online protection*, ITU, Geneva, Switzerland
- International Telecommunication Union ICT (2014). ITU ICT Indicators Database.
Available from www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Internet Live Stats (2015). 'Internet users in the world'. Available from www.Internetlivestats.com/Internet-users. Accessed 23 August 2015.
Internet Watch Foundation (2015). Available from <https://www.iwf.org.uk/>

Karunaratne, Waruni (2015). 'Fighting Cyber Crime'. *Sunday Leader*, 7 August 2015.

Livingstone, Sonia and O'Neill, Brian "Children's Rights Online: Challenges, Dilemmas and Emerging Directions", 2014.
Available from <https://arrow.dit.ie/cgi/viewcontent.cgi?article=1057&context=cserart>

Mitchell, K.J., Becker-Blease, K.A. and Finkelhor, D. (2005). 'Inventory of Problematic Internet Experiences Encountered in Clinical Practice in Professional Psychology', *Research and Practice*, Vol. 36, No. 5, pp. 498-409.
NCPA (2015). 'News, NCPA', 16 June, 2015, Available from <http://www.childprotection.gov.lk/news> Accessed 10 August 2015.

Nielsen Consumer Surveys (2014). 'Sri Lanka Year in Review'. Available from www.nielsen.com/content/dam/nielsen-global/sk/docs/2014/sri-lanka-year-in-review.pdf. Accessed 10 March 2016.

Sri Lanka, Department of Census and Statistics (2004) *Computer literacy statistics*, Department of Census and Statistics, Sri Lanka, Colombo.

Sri Lanka, Department of Census and Statistics (2006/07) *Computer literacy statistics*, Department of Census and Statistics, Sri Lanka, Colombo.

Sri Lanka, Department of Census and Statistics (2009) *Computer literacy statistics*, Department of Census and Statistics, Sri Lanka, Colombo.

Sri Lanka, Department of Census and Statistics (2014) *Computer literacy statistics*, Department of Census and Statistics, Sri Lanka, Colombo.

Sri Lanka, Department of Education Data Management Branch (2013). *Sri Lanka Education Information 2013*, Sri Lanka, Colombo, 2014.

Sri Lanka, Department of National Planning (2010). *The Emerging Wonder of Asia: Mahinda Chintana – Vision for the Future*, Department of National Planning, Ministry of Finance and Planning, Sri Lanka, Colombo.

Sri Lanka, National Child Protection Authority (2016). *History of NCPA*, NCPA, Sri Lanka, Colombo.

Srinivasan, Venkat (2014), 'Internet addiction: Real or virtual reality?' *Scientific American*, 15 May.

The Movement Against Bullying (2015). 'Bullying in Sri Lanka'.
Available from <http://nobullying.com/bullying-in-sri-lanka>.

The United Nations. (1989). Convention on the Rights of the Child. *Treaty Series*, 1577, 3.

The World Bank (2014). World Bank open data. Accessed from
<http://databank.worldbank.org/data/views/reports/tableview.aspx>

Third, Amanda, et al (2014). *Children's Rights in the Digital Age: A download from Children around the world*, Young and Well CRC, Australia, Abbotsford.

UNICEF (2014). Activating a promise, Convention on the Rights of the Children.
Available from www.unicef.org/crc/index_30160.html

UNICEF (2015). Fact Sheet: A Summary of the Rights Under the Convention on the Rights of the Children.
Available from www.unicef.org/crc/files/Rights_overview.pdf.

Wijemanne, Hiranthi (2014). Reflections on Child Rights in Sri Lanka during the Past 25 Years. Available from
www.unicef.org/crc/files/2014_CRC_6th_Op-Ed_from_Dr__Hiranthi_Wijemanne.pdf

“Keeping children in Sri Lanka
safe and empowered online”



unicef  | for every child

Published by UNICEF
ISBN: 978-955-1720-01-8
www.unicef.lk

© United Nations Children's Fund (UNICEF)
December 2017



UNICEF Sri Lanka or @UNICEFSriLanka
facebook.com/UNICEFSriLanka



UNICEF Sri Lanka or @UNICEF_SriLanka
twitter.com/UNICEF_SriLanka



unicef_srilanka
instagram.com/unicef_srilanka



UNICEF Sri Lanka
youtube.com/unicefsrilanka