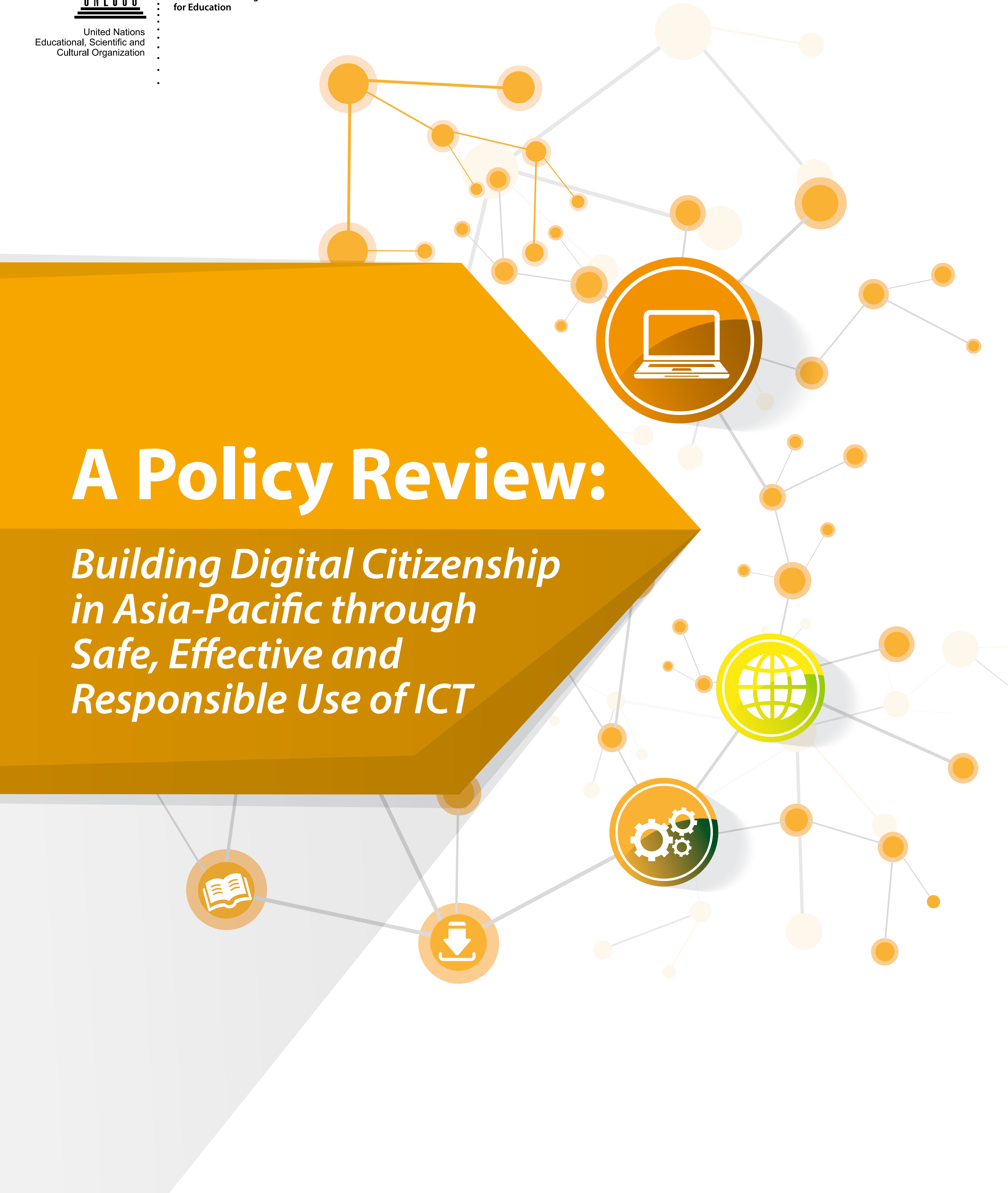
United Nations
Educational, Scientific and
Cultural Organization

UNESCO Bangkok
Asia and Pacific Regional Bureau
for Education



A Policy Review:

Building Digital Citizenship in Asia-Pacific through Safe, Effective and Responsible Use of ICT

A POLICY REVIEW:

BUILDING DIGITAL CITIZENSHIP IN ASIA-PACIFIC THROUGH SAFE, EFFECTIVE AND RESPONSIBLE USE OF ICT

Published in 2016 by the United Nations Educational, Scientific and Cultural Organization
7, place de Fontenoy, 75352 Paris 07 SP, France and UNESCO Bangkok Office

ISBN: 978-92-9223-560-4 (Print version)
ISBN: 978-92-9223-561-1 (Electronic version)

The designations employed and the presentation of material throughout this publication do not imply the expression of any opinion whatsoever on the part of UNESCO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The ideas and opinions expressed in this publication are those of the authors; they are not necessarily those of UNESCO and do not commit the Organization.

Project co-ordinators: Jonghwi Park and Maria Melizza Tan
Editor: Ellie Meleisea
Graphic designer: Umaporn Tang-on

TH/C3/EISD/16/023-500

Contents

List of figures

List of tables

List of boxes

Acronyms

CyberSAFE	Cyber Security Awareness For Everyone
EU	European Union
GNI	Gross national income
ICSC	Inter-Ministry Cyber Wellness Steering Committee
ICT	Information and communications technology
IDI	Internet development index
ITU	International Telecommunication Union
MCMC	Malaysian Communications and Multimedia Commission
NGO	Non-governmental organization
OECD	Organisation for Economic Co-operation and Development
SNS	Social networking sites
UIS	UNESCO Institute for Statistics
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICEF	United Nations Children’s Fund

Acknowledgements

Work related to this policy review was coordinated by the UNESCO Bangkok ICT in Education team, led by Jonghwi Park, the Programme Specialist. Team members include Maria Melizza Tan, Jollyn Cheong, Minju Choi, Auken Tungatarova and Danya Haseeb. The team was supported by Jian Xi Teng who conducted data analysis and contributed to writing up the report.

The team sincerely thanks the 22 participating Member States and their nominated ministries/organizations (listed in Appendix 1) for their involvement in the review, without which this study would have been impossible. It also thanks the UNESCO National Commissions for their assistance in coordinating the country participation.

The team gratefully acknowledges the contributions of the Association for the Advancement of Computing in Education (AACE) and its members, namely, Marsali Hancock, Michael Searson and Paul Resta, who provided inputs to the survey questions and technical advice on an initial analysis.

The team also appreciates the substantive feedback and comments provided by the external and internal reviewers, Brian O'Neill, Rosalie O'Neale, Misako Ito and Chantal Mairesse.

Finally, the UNESCO team extends its gratitude to Intel for its generous support and partnership that made this study possible.

Foreword

A ship in harbour is safe, but that is not what ships are built for.

– John A. Shedd

Information and communications technology (ICT) has brought numerous, unprecedented opportunities and benefits to our lives. The Internet and mobile telephone applications allow easy and quick access to people, ideas and information, link communities across continents, and boost innovation across sectors. ICT has made the world more connected, where an increasing number of people are actively using various forms of technology every day. Today, ICT is no longer an optional addition but an integral part of our lives that younger generations cannot imagine life without.

Simultaneously, however, concerns have been growing on the drawbacks and risks of using ICT. Some of the challenges include health and mental hazards, breaches in data security and safety, misuse of information, or more socially critical issues such as digital inequality, or online propaganda and radicalization. Alarming reports on the negative effects of ICT have prompted authorities to set up risk-reduction measures – as rigid as national-level content filtering and blocking. While precaution and safety are crucial factors to the general wellbeing of a society, such drastic actions have the potential to impede the full exploration and participation in the digital world that could have educational and personal value.

While it is tempting to assume that risks can be mitigated and prevented concurrently with ensuring maximized and uninhibited opportunities, the truth is that opportunities and risks are two sides of the same coin. A growing body of research suggests that although learners who seek opportunities in the digital space do face greater risks, they are also able to learn to cope with them, in which case the benefits they gain can ultimately outweigh the risks. However, it is also evident that the line between risk and danger can be thin, potentially exposing learners to detrimental consequences, such as trauma and an overall unfavourable experience in the digital world.

The Education 2030 Agenda identifies the acquisition of ICT skills as an essential requirement for citizens to confidently thrive in this rapidly evolving society. Considering that ICT is the dominant means by which we can participate in and contribute to the knowledge society, it is of paramount importance that citizens are equipped with the appropriate knowledge, skills and attitudes. Users need to learn to leverage and enjoy the countless benefits of using ICT while also becoming resilient in the face of potential risks.

In this regard, the UNESCO Asia and Pacific Regional Bureau for Education (UNESCO Bangkok) launched the "Fostering Digital Citizenship through Safe, Effective and Responsible Use of ICT" project. It aims to promote policy dialogue on building the education sector's capacity in setting up safe digital environments for children as well as in educating children to be resilient, effective and responsible users of ICT.

This report is a major output of the project. The policy review described in this report took stock of national policies in 22 Member States in the Asia-Pacific region and assessed the capacity of their education sectors to foster digital citizenship among children aged 0-18. It is encouraging to note from the study that surveyed Member States' policies to promote ICT opportunities mature alongside policies that address potential risks, at varying levels of policy maturity. However, while the surveyed Member States recognize the importance of equipping children with ICT skills and providing basic infrastructure, the findings indicate that there is much to be done for young learners (e.g. early childhood education and lower primary education) in introducing the concept of safe, effective and responsible use of ICT to their national curriculum as well as to their teacher professional development programmes.

We trust that this report will inform the Member States on the importance of this aspect in the education systems, and will serve as an impetus for education stakeholders in the region to explore, discuss and develop policies, relevant programmes and further research towards promoting children's safe, effective and responsible use of ICT.

Gwangjo Kim

Gwang-Jo Kim
Director
UNESCO Bangkok

Executive summary

This report presents the results of a policy review that examined the national policies, initiatives and efforts of Member States in the Asia-Pacific region relating to the promotion of safe, effective and responsible information and communication technology (ICT) environments and ICT use by children. In particular, the review focused on national education policies relating to fostering digital citizenship in schools and among students, teachers, parents and caregivers.

This policy review was conducted as part of UNESCO's "Fostering Digital Citizenship through Safe, Effective and Responsible Use of ICT" project.

Methods

As the focus of this policy review was on the national-level policies of Member States, the main source of primary data was a pioneering survey among representatives of Asia-Pacific Member States. These representatives were national experts or government officials who were officially nominated by their respective National Commissions for UNESCO.[1]

In addition to a survey, the policy review process involved collecting and analysing case studies of national initiatives that seek to foster an ICT environment that is not only safe but also conducive to learning, which entails balancing policies for risk reduction with policies that maximize the opportunities and benefits of ICT.

The policy review had four main components:

1. A survey of national representatives.
2. A review of relevant national initiatives.
3. An analysis of the survey data regarding national policies and practices, with the aim of identifying good practices and highlighting any gaps that need to be addressed.
4. The development of policy recommendations for Member States.

The target audiences of this policy review are policy-makers in the Asia-Pacific region, stakeholders in the ICT and education sectors, civil society, and development partners and organizations. The findings of this policy review will serve as the primary reference for UNESCO's "Policy Guidelines on Fostering Digital Citizenship through Safe, Effective and

[1] A total of 22 Member States out of the 46 Member States contacted responded to the survey.

Responsible Use of ICT for children in the Asia-Pacific region", which aim to guide Member States in developing policies and initiatives that respond to the issues in their particular contexts.

Key findings

The key findings of the policy review were as follows:

- **Member States recognize the importance of equipping children with ICT skills and providing basic infrastructure.**

  The ministries of education in about 75 per cent of the participating Member States have policies promoting basic ICT literacy skills among children and also have policies promoting at least one computer lab per school at the secondary school level. However, the Member States give less attention to training beyond basic ICT literacy. More advanced ICT skills would promote more sophisticated media and information literacy, such as interactive and critical use of media as well as constructive online participation and content creation.

- **A multi-sector approach is taken by many Member States in the development of cyber safety or privacy policies, but it could be further improved.**

  Two-thirds of the participating Member States have involved experts from one or more of four key sectors (law enforcement, health, education and cyber security) in the development of cyber safety and privacy policies. But recent research indicates that Member States should create a dialogue that also includes children's perspectives on the opportunities and risks of ICT use and increasing digital literacy skills, while developing digital citizenship values.

- **Policies need to be improved in supporting teachers to be adequately equipped to teach with ICT.**

  Overall, the policies that most of the surveyed Member States have implemented to support the development of teachers' basic ICT skills, alongside cyber wellness and cyber security competencies, can be improved. Furthermore, most teacher development policies relating to ICT use are not fully implemented. Without the basic knowledge and skills to use ICT and to utilize ICT in teaching, teachers cannot be effective in nurturing students to be active digital citizens who use ICT safely, effectively and responsibly.

- **Member States' policies to promote ICT opportunities mature alongside policies that address potential risks.**

  Survey responses show that a Member State's policy readiness to empower children to embrace ICT opportunities is strongly and positively correlated with its policy readiness to address potential risks ($r > 0.9$). It is evident among surveyed Member States that opportunity-oriented policies and safety-oriented policies go hand in hand.

- **Member States focus on children in secondary school, much less on younger children.**

  Only around half of the participating Member States have policies to promote basic ICT skills and digital citizenship among children aged 0-8 years old. Furthermore, many countries have not established the technical infrastructure required to facilitate access and use of ICT among younger children.

- **Half of the Member States lack security measures and therefore have vulnerable school ICT systems.**

  Only 55 per cent of the participating Member States have policies in place for secure WiFi, networks and encryption at the secondary school level, while only 48 per cent have such policies at the early childhood to early primary school age group level and 51 per cent have them at the primary school age group level. These findings suggest that a significant number of school ICT systems in the Asia-Pacific region are vulnerable to malicious attacks or unauthorized intrusions; thus the storage and transmission of private information is at risk. School-based ICT systems are potentially vulnerable to malicious attacks targeting students' personal information and data.

- **Audits and reviews of school ICT security systems are lacking.**

  Over 60 per cent of the participating Member States lack policies to enable schools to regularly review and audit the safety and security of their ICT systems. This could potentially lead to unauthorized intrusions or malicious attacks.

- **Most Member States in the Asia-Pacific region block content and place restrictions on access to content.**

  More than 80 per cent of the participating Member States employ content filtering systems and/or monitoring systems at the local, provincial and/or national levels. These Member States view these systems as being necessary for reducing the risks of ICT use among children.

- **Most Member States lack systems for monitoring and evaluating digital citizenship policies and procedures.**

  Monitoring and evaluation of programmes is an important aspect of evidence-based policy creation and implementation. However, 73 per cent of the Member States that participated in the survey do not have assessment systems in place to measure the efficacy of their digital citizenship policies and procedures. Furthermore, while 85 per cent of the Member States have an education management information system (EMIS) in place, only 40 per cent of those Member States use the EMIS to manage information relating to students' cyber safety.

- **The needs of the Member States in the Asia-Pacific region are diverse.**

  The findings reinforce the results of other research regarding the vast disparity and variation seen in Asia-Pacific with regard to ICT technical resources, infrastructure capabilities and integration of ICT into education. The findings of the survey also demonstrate that Member States in the Asia-Pacific region occupy the entire spectrum of national ICT policies in terms of "leadership and accountability", "education" and "technical infrastructure" – ranging from Member States that have no policies (i.e. Level 0) relating to the survey's three research categories to Member States that have policies that are not only implemented but are also monitored and evaluated (i.e. Level 3).

- **Member States lack adequate data on children's behaviour, perceptions and usage of ICT both nationally and regionally.**

  There is a lack of research establishing the baseline ICT usage among children or about their online behaviour, the quality and nature of children's ICT use when in school, or ICT use among family members and in the wider community. Almost half (47 per cent) of the participating Member States do not have a national programme to promote the use of research to inform and support policy, and if one is in place, it is not used consistently. The lack of research and locally-relevant data indicates that policies are developed based on assumptions or on research that may not be locally applicable.

Policy recommendations

While the Member States have differing capacities to develop and implement their digital citizenship policies, the following policy recommendations can aid policy-makers in focusing their efforts.

- **Take a balanced approach to ICT.**

  Member States should develop national policies for ICT in education that foster digital citizenship in schools, maximize the opportunities afforded by ICT and facilitate the development of ICT infrastructure. At the same time, Member States should employ ICT-related policies that mitigate risks and enhance safety for children.

- **Develop basic ICT skills in all children.**

  Member States should institute and implement policies that increase ICT literacy skills among children of all age groups (from 0-18 years old), and provide the technical infrastructure to facilitate such learning.

- **Go beyond basic ICT skills.**

  Member States should develop and implement education policies that increase provisions for gaining more advanced, higher-order ICT skills, through curricular and extra-curricular activities, so as to enable learners to cope with the changing digital environment. UNESCO's extensive resources on Media and Information Literacy may serve as useful references on this.

- **Develop appropriate technical infrastructure for early childhood education.**

  Member States should develop and implement education policies and age-appropriate technical infrastructure to increase opportunities for young children (0-8 years old) to access and use ICT.

- **Incorporate digital citizenship as part of teacher competency standards.**

  Member States can complement their student-focused policies by developing and implementing competency standards that ensure teachers are equipped with basic ICT skills and therefore have the capacity to teach children about safe, effective and responsible ICT use and digital citizenship. In addition, Member States should support policies that build teachers' capacity to utilize ICT in teaching, so as to increase the opportunities afforded by ICT in schools.

- **Improve the allocation of resources to the security of ICT systems.**

  Member States should ensure that sufficient resources, in terms of budget, personnel and training, are allocated to providing adequate security measures for school-based ICT systems.

- **Establish a nationwide EMIS to improve monitoring and evaluation in relation to digital citizenship.**

  A nationwide EMIS with a built-in learning log analytics will serve as an essential element in understanding and monitoring students' digital behaviour and thus support the development of an effective and data-driven digital citizenship programme for children.

- **Adapt programmes and initiatives to local contexts.**

  Member States should develop policies that are adapted to national and local contexts and tailored to the needs of the local children.

- **Pursue a multi-stakeholder, multi-sector approach.**

  Member States should consider pursuing public-private partnerships as part of a multi-stakeholder, multi-sector approach that incorporate various perspectives to developing and implementing policies and initiatives relating to children's safe, effective and responsible use of ICT.

1. Introduction

The proliferation of ICT and their ubiquitous nature have made them an indispensable part of our daily lives and have fundamentally changed the way in which our societies operate. Without a doubt, the opportunities and benefits that ICT has brought to our lives are tremendous. ICT has undeniably revolutionized the way we learn, travel, work, engage and interact with one another, overcoming limitations set by distance, time and other contextual barriers.

In recent years, some forms of ICT, such as mobile telephones, have become affordable for everyone and are today allowing easy access to information, people, services and goods. As of the end of 2014, there were almost 7 billion mobile telephone subscriptions globally, with around 4.5 billion unique subscribers and about 3 billion people (40 per cent of the world's population) had internet access via mobile and/or fixed broadband subscriptions (International Telecommunication Union, 2015a).

At the time of the conception of the Millennium Development Goals (MDGs) "the international community was only beginning to recognize the catalytic potential" of ICT to advance development agendas and priorities (United Nations Economic and Social Council, 2015, p. 9). Since then, ICT has been recognized as a vehicle to promote, enable and support the three pillars of sustainable development, namely social development, economic development and environmental protection. Accordingly, the Education 2030 Agenda highlights ICT as a means "to strengthen education systems, knowledge dissemination, information access, quality and effective learning, and more effective service provision" (UNESCO, 2015a, p. iv). Furthermore, the Education 2030 Framework for Action emphasizes ICT skills as a necessary skill set that citizens should acquire to confidently thrive in our globalised, knowledge-based and technology-driven world.

In as much as digital technologies have brought about significant opportunities and benefits, they have also raised an array of social and ethical issues. Such issues include online safety and security, misuse of information, and health and mental hazards. The Asia-Pacific region has not been exempt from cases of ICT abuse in the form of spamming, data theft, intellectual property infringement (plagiarism and piracy), delinquency, health and wellness issues, excessive exposure to online games, cyber bullying, fraud, identity theft, pornography, sex trafficking and radicalization. In response, public anxiety has been raised – particularly when children and adolescents are affected. This has prompted some groups to propose censorship or strict regulation of ICT use or of internet access.

These concerns are evident in UNESCO ICT in Education forums. While recognizing the benefits of using ICT in education, stakeholders from various Member States, institutions, organizations and schools have expressed their concerns about the risks and drawbacks of using such technology. Demand has grown for research, policy responses, advocacy programmes, capacity building and corresponding resources. There is a sense of urgency for the education sector to secure expert guidance, along with models of effective measures.

Reflecting this sense of urgency, researchers from Europe and Member Countries of the Organisation for Economic Co-operation and Development (OECD) have put their collective efforts into understanding children's online behaviour and forming evidence-based policies to mitigate the risks of using ICT in education, without diminishing the benefits (Livingstone et al., 2011; OECD, 2012a; O'Neill, 2014). Accordingly, most of the relevant research has been carried out in the context of industrialized Western nations, i.e. in Europe and Northern America. However, research is also needed in other regions, including the Asia-Pacific, in order to identify ways to address issues given the characteristics and contextual factors in the region, especially those in the developing and emerging countries (Gasser et al., 2010). In particular, research is needed to address the gap in data relating to how children below 15 years olds use ICT.

In response to this, the UNESCO Asia and Pacific Regional Bureau for Education (UNESCO Bangkok), with support from Intel, carried out a policy review that took stock of current national policy responses to the issues relating to ICT use and assessed the education sector's readiness and capacity in fostering digital citizenship among children aged 0-18. Specifically, the review sought to answer the question: How ready are governments in the region to provide environments that enable our young generation to be safe, effective and responsible users of ICT?

The policy review was conducted as part of the "Fostering Digital Citizenship through Safe, Effective and Responsible Use of ICT" project and had four components:

- A survey of national representatives to gain information about national policies and initiatives relating to ICT use in education by children aged 18 and under.
- A review of national initiatives to collect relevant data on initiatives to promote a safe and opportunity-rich ICT environment, including legislation, regulations, national curricula and education programmes.
- An analysis of the national practices, with the aim of identifying good practices in fostering a favourable environment for children's responsible and safe use of ICT and highlighting any gaps.
- Development of policy recommendations for Member States, based on the data analysis.

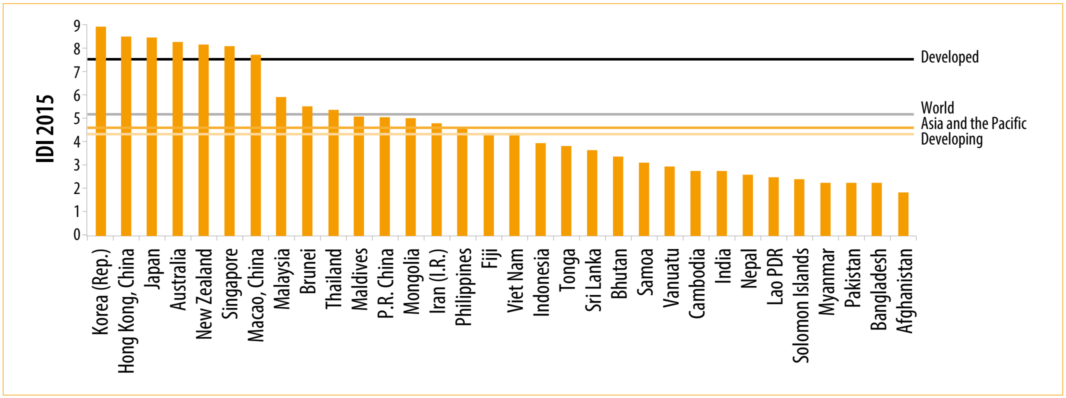
2. Background

2.1. ICT development in the Asia-Pacific region

The Asia-Pacific region covers a vast geographical area encompassing a wide diversity of cultures, languages, religions, ethnicities and histories. The Member States not only differ from each other but often also have significant diversity within their countries. These differences are important considerations as a person's ethnicity and socio-economic status affects his or her opportunities and risks, including those related to ICT use.

The International Telecommunication Union (ITU) has ranked Asia-Pacific as the most diverse region in the world in terms of ICT development (ITU, 2015b). In 2015, six of the top 20 countries ranked in the ICT Development Index (IDI) were from the Asia-Pacific region, namely, Australia, Hong Kong, Japan, New Zealand, Korea (Rep.) and Singapore. That year, four of the least ICT-developed countries (those below the 140th rank in the IDI) were also from the Asia-Pacific region, namely, Myanmar, Pakistan, Bangladesh and Afghanistan. Figure 1 shows the wide range of IDI values in the region.

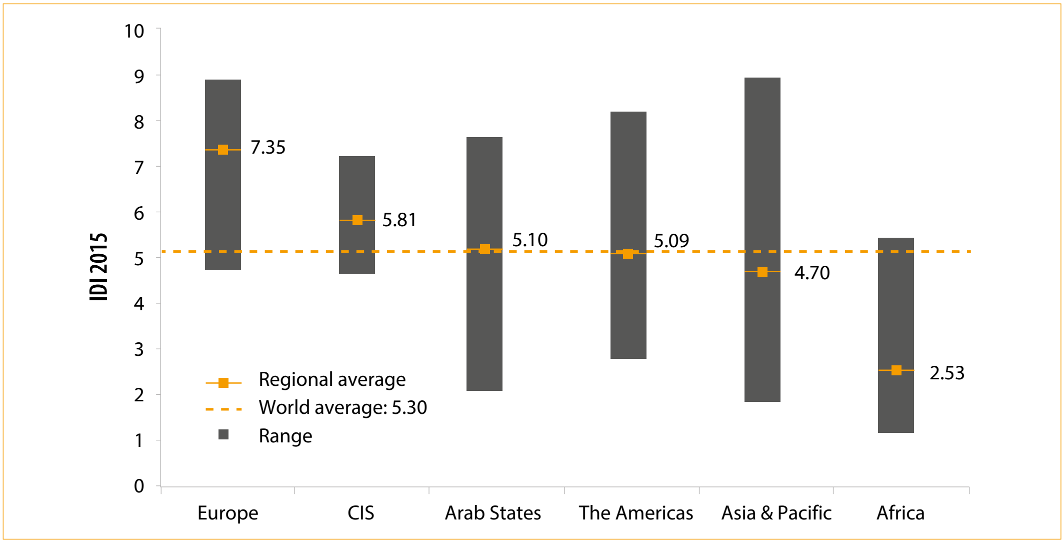
Figure 1: IDI values in the Asia-Pacific region, 2015



Source: ITU, 2015b

Furthermore, given the large number of countries in the Asia-Pacific region with limited access to the internet, the average IDI score of the region was below the world average (Figure 2).

Figure 2: IDI by region compared with the global average, 2015



Source: ITU, 2015b.

There are also varying levels of economic development in the region. Some of the region's countries are among the highest-income countries in the world, including Australia, Japan and Singapore, while the region also has some of the lowest-income countries, such as Nepal and Afghanistan. Table 1 illustrates the diversity of the Member States that responded to the survey, listing their IDI rankings and Gross National Income (GNI) levels as indicators of ICT development and economic development, respectively.

Table 1: Participating Member States' IDI rankings and GNI per capita

Country	Asia-Pacific sub-region	IDI 2015 Rank	Income classification based on GNI per Capita	GNI per capita ($)
Commonwealth of Australia	Pacific	13	High Income	64,540
Republic of Singapore	Southeast Asia	19	High Income	55,150
Japan	East Asia	11	High Income	42,000
Brunei Darussalam	Southeast Asia	71	High Income	37,320
New Zealand	Pacific	16	High Income	31,890

Country	Asia-Pacific sub-region	IDI 2015 Rank	Income classification based on GNI per Capita	GNI per capita ($)
Republic of Korea	East Asia	1	High Income	27,090
Cook Islands	Pacific	Unranked	High Income (GDP per capita as of 2012)	18,782
Niue	Pacific	Unranked	Upper Middle Income (GDP per capita as of 2011)	15,066
Republic of Kazakhstan	Central Asia	58	Upper Middle Income	11,850
Federation of Malaysia	Southeast Asia	64	Upper Middle Income	11,120
Republic of Palau	Pacific	Unranked	Upper Middle Income	11,110
People's Republic of China	East Asia	82	Upper Middle Income	7,400
Mongolia	East Asia	84	Upper Middle Income	4,280
Independent State of Samoa	Pacific	122	Lower Middle Income	4,060
Federated States of Micronesia	Pacific	Unranked	Lower Middle Income	3,200
Kingdom of Bhutan	South & West Asia	119	Lower Middle Income	2,370
Republic of Uzbekistan	Central Asia	115 (2014)	Lower Middle Income	2,090
Solomon Islands	Pacific	139	Lower Middle Income	1,830
Lao People's Democratic Republic	Southeast Asia	138	Lower Middle Income	1,660
People's Republic of Bangladesh	South & West Asia	144	Lower Middle Income	1,080
Federal Democratic Republic of Nepal	South & West Asia	136	Low Income	730
Islamic Republic of Afghanistan	South & West Asia	156	Low Income	680

Sources: World Bank, ITU, Australian Department of Foreign Affairs and Trade, Cook Islands Ministry of Finance and Economic Management.

Note: The official names of Member States were used in this table. For subsequent mentions, the shortened names will be used.

The diversity in the region has presented challenges in terms of providing recommendations for policy improvements that apply across the region. Despite this diversity, however, there are certain general policies that can be applied in most countries in the region to foster children's safe, effective and responsible use of ICT.

ITU data indicate that mobile internet 2G covers 95 per cent of the world's population and that mobile broadband subscriptions grew twelve-fold between 2007 and 2015, and now cover almost half (47 per cent) of the world's population. Due to the rapid development of affordable mobile technology and the progress in mobile internet penetration, ICT use is also increasing quickly in the Asia-Pacific. As of 2015, over a third (39 per cent) of households in the Asia-Pacific region had internet access, with 36.9 per cent of individuals using the internet, while mobile broadband subscriptions stood at 42.3 per cent. Furthermore, in 2015 the region had an estimated 1.5 billion people using the internet as well as 1.7 billion active mobile broadband subscriptions and 3.7 billion mobile cellular subscriptions (ITU, 2015a).

This greater accessibility to ICT has implications for education. The integration of ICT into social and economic spheres necessitates the development of digital literacy. This would support children's education at the primary, secondary and tertiary levels, and would facilitate lifelong learning (UNESCO Institute for Statistics, 2014).

International benchmarking studies indicate that much progress is needed to integrate ICT into education. A European study titled *Survey of Schools: ICT in Education*, found that students' ICT use in the classroom lags far behind use outside school, affecting students' confidence in their digital competencies (European Commission, 2013). Studies also indicate that boosting teacher professional development improves ICT use in the classroom. Hence, countries need to develop specific policies to support and guide the use of ICT in teaching and learning.

In the Asia-Pacific region, the policy-making process differs between the Member States, with some Member States developing policies at the central level, under the responsibility of one agency that later coordinates the implementation of actions and initiatives, while other Member States have a more complex policy-making process involving interactions between ministries, agencies and other stakeholders.

This diversity in processes is also seen in other regions. For example, the European Commission (EC) reported in 2012 that European Union (EU) Member States take different approaches to the development of national internet and ICT policies and to the implementation of actions and initiatives targeted toward children (European Commission, 2014).

While evidence-based policy making requires research addressing the specific issues arising from children's use of ICT and the fostering of digital citizenship values and skills, such research is often lacking in the Asia-Pacific region. In particular, in-depth studies on the state of ICT policies regarding digital citizenship and the characteristics of children's ICT use, similar to the EU Kids Online and related studies, are uncommon in the Asia-Pacific region (UNESCO, 2015b).

2.2. Digital citizenship

In many countries, policy-makers' understanding of ICT in children's education has evolved from a focus on minimising the risks of ICT towards the view that supports building awareness and critical thinking skills in students so as to ensure they use ICT effectively and responsibly. The latter approach is one that supports "digital citizenship". Policy-makers in Britain, for example, have found that the challenges brought about by unregulated access to ICT and online content can only be addressed if policies move beyond building children's digital skills and ICT literacy to encompass the responsible use of ICT by critical, ethical and empowered children (Department for Children, Schools and Families, 2008). This approach is being implemented in Europe through transforming the Safer Internet Programme into the Better Internet for Kids Programme (European Commission, 2012).

This is relevant to the policy debate relating to hate speech and online radicalisation, which are linked to the spread of terrorism. Digital citizenship programmes seek to impart values and concepts that enable children and youth to critically evaluate the information they are given by the people wishing to radicalise them. This approach recognises that reducing the appeal of extremist messages can best be achieved through strengthening the capacity of children and youth to evaluate online content critically (International Centre for the Study of Radicalisation and Political Violence, 2009).

Organizations have defined "digital citizenship" (also known as "media and information literacy", "digital literacy" and "information literacy") in various ways. Ongoing policy development within UNESCO has led to a broader understanding of this concept, going beyond media-related skills to encompass cognitive, critical and creative abilities. Accordingly, UNESCO defines "media and information literacy" as a set of competencies that empower citizens to access, retrieve, understand, evaluate and use, create and share information and media content in all formats using various tools in a critical, ethical and effective way, in order to participate and engage in personal, professional and societal activities (Wilson et al., 2011).

In *Digital Citizenship in Schools,* "digital citizenship" is defined as "the norms of appropriate, responsible behaviour with regard to technology use" (Ribble, 2016) and is perceived as encompassing nine elements: digital access, digital commerce, digital communication, digital literacy, digital etiquette, digital law, digital rights and responsibilities, digital health and wellness and digital security.

The Open University of UK defines "digital literacy" as the ability to find and use information, but notes that it also encompasses skills in communication, collaboration and teamwork, social awareness in the digital environment, understanding of e-safety and creation of new information. According to this definition, digital literacy is underpinned by critical thinking and evaluation (The Open University, 2012).

The International Society for Technology in Education sets out its digital citizenship standards for students and teachers (ISTE, 2016) as follows:

Students should:

- Understand human, cultural and societal issues related to technology and practice legal and ethical behaviour.
- Advocate and practice safe, legal and responsible use of information and technology. Exhibit a positive attitude toward using technology that supports collaboration, learning and productivity.
- Demonstrate personal responsibility for lifelong learning.
- Exhibit leadership for digital citizenship.

Teachers should:

- Understand local and global societal issues and responsibilities in an evolving digital culture and exhibit legal and ethical behaviour in their professional practice.
- Advocate, model and teach safe, legal and ethical use of digital information and technology, including respect for copyright, intellectual property and the appropriate documentation of sources.
- Address the diverse needs of all learners by using learner-centred strategies, providing equitable access to appropriate digital tools and resources.
- Promote and model digital etiquette and responsible social interactions related to the use of technology and information.
- Develop and model cultural understanding and global awareness by engaging with colleagues and students of other cultures using digital-age communication and collaboration tools.

The concept of digital citizenship for children has been set within a rights-based framework, emphasizing the right of children, in particular, to benefit from the fullest exercise, enjoyment and participation in society through the use of ICT. This has featured strongly in various global forums, including in the United Nations Committee on the Rights of the Child, in a report by the United Nations Special Rapporteur for Freedom of Expression (2014), in the Internet Governance Forum (Livingstone et al., 2016) and in the Council of Europe (2012).

Taking off from the foregoing discussion, for purposes of this policy review, "digital citizenship" is defined as "being able to find, access, use and create information effectively; engage with other users and with content in an active, critical, sensitive and ethical manner; and navigate the online and ICT environment safely and responsibly, while being aware of one's own rights."

3. Methods

The policy review was a quantitative study that compiled information relating to the scope and comprehensiveness of Member States' national policies for: the safe, effective and responsible use of ICT by children; fostering digital citizenship in children; and providing schools with the required technical infrastructure. The review also examined practices at the national level that have successfully promoted children's safe, effective and responsible use of ICT.

3.1. Data sources

The main source of the data for this policy review was a survey. The survey was conducted between 19 May and 15 August 2015. All 46 Member States in the Asia-Pacific region were invited to participate and 22 Member States accepted. The participants in the survey were national experts or officials who were officially nominated by their respective National Commissions for UNESCO. A list of the participating Member States can be found in Appendix 1.

The survey was administered in English. Given that English was not the native language of many of the participants, key technical terms in the survey were assessed during the preparation stage to ensure that they would be understood correctly. The technical terms were assessed by faculty and students from two universities in the United States. These assessors, whose native languages are those spoken in the Asia-Pacific region, read the survey and highlighted any terms that were confusing or unclear. This process led to the inclusion of the definitions of five key terms at the beginning of the survey to ensure uniform understanding of these terms. For the benefit of participants from Central Asia, the survey was translated into Russian. None of the survey participants reported any confusion over the terms.

The survey was administered in electronic and hardcopy formats, and the participants were able to choose their preferred format.

In addition to conducting the survey, information was derived from analysing reports and resources prepared by international organizations, non-governmental organizations (NGOs), research centres, research groups and other bodies, including private companies.

The team also sought verbal inputs from policy-makers, experts, representatives of NGOs and the ICT industry, and students (regional consultation conducted in September 2015). They also examined national initiatives that have successfully promoted the safe, effective and responsible use of ICT by children, and compiled case studies on these initiatives.

3.2. Survey questions

The survey contained questions on national policies and practices in three categories: leadership and accountability, education, and technical infrastructure. For the full survey instrument, please see Appendix 2.

Leadership and accountability

The questions in this category examined the extent to which each Member State had taken national policy actions and had committed to promoting the safe, effective and responsible use of ICT by children. In particular, these questions examined the extent to which Member States had articulated a commitment to digital citizenship and cyber wellness such that school systems had recognised and implemented these elements as components in their curricula and school culture. This category was divided into three sub-groups: national campaigns, stakeholder involvement, and management and budget.

Questions included those about whether the Member States had implemented campaigns to promote the safe and responsible use of ICT as well as to discourage ICT abuse and misuse; about whether subject experts had been involved in the development of policies; and about whether national resources had been allocated to efforts promoting children's safe, effective and responsible ICT use.

Education

The questions in this category focused on policies which target the various stakeholders in children's education, including school leaders, teachers, caregivers and students. The questions also examined whether the concepts of digital citizenship and cyber wellness had been integrated into learning opportunities for students and teachers.

The survey participants were asked to differentiate their responses according to the following grade levels:

- Early childhood and early primary (for children aged 0-8).
- Primary school (for children aged 9-12).
- Secondary school (for children aged 13-18).

Technical infrastructure

The questions in this category examined efforts at the national level to build sound technical infrastructure in the education sector to promote the safe, effective and responsible use of ICT by children and to create environments conducive to digital citizenship and cyber wellness. In particular, the questions enquired about technical resources and the capabilities of schools, including computer lab to student ratio, internet bandwidth, school audits and reviews of security systems, and monitoring and evaluation mechanisms. The survey participants were asked to differentiate their responses according to the same age groups listed under the education category.

The survey contained 121 questions that gave the participants a response scale (see below), and 11 short-answer questions, in total 132 questions (Table 2).

Table 2: Format of the survey

	Domains and topics	Number of Questions
1	**Leadership and Accountability**	10
	National campaigns	2
	Stakeholders' involvement	4
	Management and budget	4
2	**Education**	84
	Early childhood to early primary (0-8 years old)	28
	Primary (9-12 years old)	28
	Secondary (13-18 years old)	28
3	**Infrastructure**	27
	Early childhood to early primary (0-8 years old)	9
	Primary (9-12 years old)	9
	Secondary (13-18 years old)	9
4	**Short-answer items**	11
	Total	**132**

The response scale permitted the participants to indicate the degree of policy readiness for each response.

Level 0: No policy is in place.
Level 1: A policy is in place but not implemented in practice.
Level 2: A policy is in place and is also being implemented.
Level 3: A policy is implemented and subject to monitoring and evaluation.

The responses from each participant were averaged to quantify each country's overall level of policy readiness in each survey category. This facilitated an understanding of the state of policy in each participating Member State as well as enabling the identification of any gaps between policy and practice. Please refer to Appendix 3 for a summary of the full set of responses given by the participants.

3.3. Internal reliability

Analysis of the survey results found that the responses are internally consistent, implying the strong internal reliability of the survey items. As shown in Table 3, each of the three categories had a high Cronbach's alpha coefficient (α=0.947 to 0.993), as did the sub-groups of questions within each category (α=0.922 to 0.988).

Table 3: Internal reliability of the survey responses

	Categories and sub-groups	Cronbach alpha
1	**Leadership and accountability**	0.947
	National campaigns	0.972
	Stakeholders' involvement	0.922
	Management and budget	0.945
2	**Education**	0.993
	Early childhood to early primary (0-8 years old)	0.985
	Primary (9-12 years old)	0.987
	Secondary (13-18 years old)	0.988
3	**Infrastructure**	0.983
	Early childhood to early primary (0-8 years old)	0.967
	Primary (9-12 years old)	0.961
	Secondary (13-18 years old)	0.958
4	**Short-answer questions**	n.a.

3.4. Limitations

The self-reporting nature of the survey lent itself to possible biases. While the nominated local education experts or officials were requested to validate their responses with the relevant ministries or colleagues for specialist areas such as early childhood education and technical infrastructure, the responses may have been subject to recall failure and consistency-seeking behaviour.

Another challenge arising from the self-reporting survey method of collecting data is that some participants did not respond to all of the questions in the survey. This was generally because they were unable to obtain the necessary information or because they did not wish to divulge confidential information. For a few cases, the observance of government bureaucratic requirements prevented respondents from submitting the survey.

In addition, where multiple respondents from the same Member State participated in the survey, the respondents sometimes gave conflicting responses. The responses were factual rather than subjective, so different participants from the same country (typically from different ministries) may have had differing knowledge of the policies.

In rare cases where multiple responses to a survey question were received from a Member State, the responses were aggregated into one overall survey response per Member State to ensure equal weight for each Member State's response. Where different scores were provided under one policy question, the highest score was recorded.

A related issue was that while there was some follow-up to clarify facts, time and cost considerations made it impossible to extensively verify the information provided in the survey responses. No documentary evidence was requested from the participating Member States. These issues warrant follow-up studies that will further look into background information in support of the survey responses.

A further challenge that may have affected the validity of the responses was the lack of a common understanding among the respondents on key concepts such as cyber wellness, digital citizenship, children's safe and responsible use of ICT. Furthermore, there may have been some confusion over what was meant by the word "policy". The wide range of actions covered by this survey required the use of the term "policies" as a catch-all term to cover all policies, programmes, resources, actions and initiatives that Member States use to further their goals for children's digital citizenship and to foster the safe, effective and responsible use of ICT. In view of this possibility, the indicators used and the findings of the survey may not be comparable with data and statistics from other research bodies.

In terms of scope, the focus of the study was national education policies affecting children aged 18 and under in the formal education system in the Asia-Pacific region, thus the scope of the survey was limited to policies affecting the formal school system. Accordingly, the findings cannot be extrapolated to non-formal education.

Given that fewer than half of the Member States in the region, 22 out of a total of 46, provided responses to the survey, the findings cannot be generalized to all countries in the region. Furthermore, since Member States differ in their methods of developing and applying national policies, these differences must be taken into account when assessing how the findings apply to any other Member State.

Furthermore, an issue affecting the reliability of the statistics in this report is that it was not always possible to meet the conventional sample size requirements for statistical validity.

4. Survey findings

4.1 Leadership and accountability

4.1.1. Who is involved in developing cyber safety and privacy policies?

A Member State's capacity to develop effective cyber safety or privacy policies can be assessed by examining whether experts from multiple sectors are involved in such policy development. This is also a measure of the government's commitment to policy action on this issue. To evaluate this, the survey question asked to what extent personnel from various sectors were involved in the development of cyber safety and privacy policies.

The responses indicate that many of the participating Member States take a multi-sector approach, involving various government bodies in the development of cyber safety and privacy policies. That is, when developing cyber safety and privacy policies, they seek expert advice from at least one of the four key sectors related to such policies: health, education, law enforcement and cyber security.

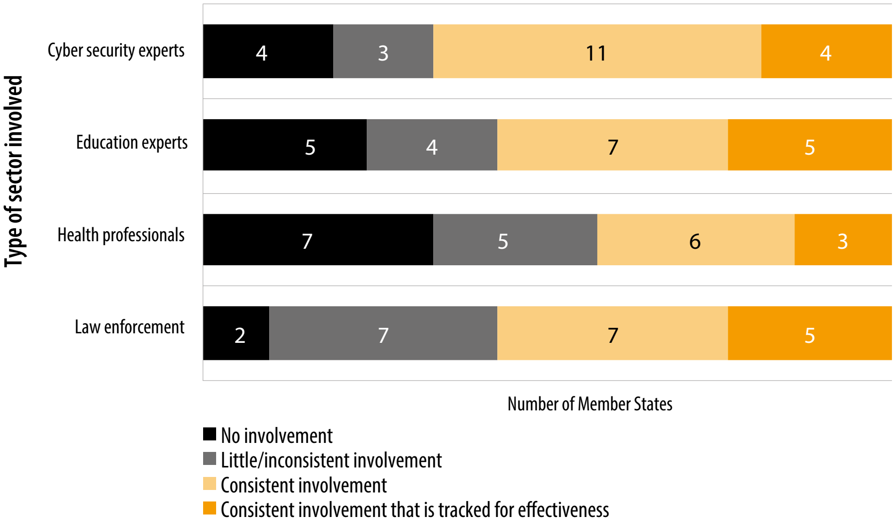
The survey responses indicate that a third of the participating Member States involve experts from all of the four sectors in the development of their cyber safety and privacy policies. These Member States include Malaysia, New Zealand, P.R. China, Korea (Rep.), Samoa, Singapore and Uzbekistan. The remaining two-thirds of the participating Member States involve between one and three of the four sectors, seeking advice from a combination of law enforcement personnel, health professionals, education experts and cyber security experts. About 80 per cent of the participating Member States involve at least two of the four sectors. Thus, the findings suggest that most of the Member States feel it is necessary to take a multi-sector approach in developing cyber safety or privacy policies.

The participating Member States generally consider advice from the law enforcement sector as being more important than advice from other sectors when developing cyber safety and privacy policies. More than 90 per cent of the Member States surveyed involve law enforcement personnel in the development of cyber safety and privacy policies. About 80 per cent of the participating Member States also involve cyber security experts in the development of such policies. In contrast, health professionals are the least involved, as about 24 per cent of the participating Member States have little or inconsistent involvement and about 33 per cent have no involvement of health professionals in the development of cyber safety or privacy. Thus, the survey responses indicate that governments in the region focus primarily on law enforcement and cyber security expertise over health and education expertise when developing cyber safety and privacy policies.

The survey responses indicate that regardless of the large differences in their levels of ICT development and income levels, most of the participating Member States involve experts in this type of policy-making. However, the intensity of involvement varies from state to state. Member States with higher income levels report greater and more consistent involvement of law enforcement and cyber security experts in such policy-making.

Figure 3 illustrates the Member States' responses regarding the involvement of experts from the four sectors in the development of cyber safety and privacy policies.

Figure 3: Number of Member States that involve the various sectors in developing cyber security and privacy policies, by type of sector



Note: Japan was unable to submit responses to these survey questions.

The survey responses suggest that the current ICT policy agenda of Asia-Pacific Member States, which emphasises security, is consistent with policies in other regions. Many researchers believe, however, that this emphasis is not conducive to beneficial outcomes for children. The focus on protection against online risks without an equal emphasis on risk prevention through children's education, can lead to a situation in which the benefits of ICT are diminished but safety has not actually been improved. Some researchers consider that such policies have led to a situation in which "children in many parts of the world today have inherited a popular discourse that is characterised primarily by fear" (Third et al., 2014, p. 40). In fact, the success of cyber safety campaigns has meant that "risk and safety tend to dominate children's sense-making about their digital media practices" (Third et al., 2014, p. 42). They believe that children need to not only be aware of risks and how to articulate them, they must also learn how to translate what they know into "behaviour change that enables children to navigate risks safely" (Third et al., 2014, p. 42). Therefore, Member States should not just focus on the message of awareness and safety when developing policies relating to such issues. Accordingly, although it is necessary to involve law enforcement and cyber security experts in the development of cyber safety and privacy policies, advice should also be sought from experts in the education and health sectors.

Member States should aim to develop policies that seek to empower children to use ICT in a safe, effective and responsible way, through digital citizenship education. To ensure balanced policies, Member States could consider incorporating the advice of children (Third et al., 2014) and creating a dialogue that includes children's voices and perspectives regarding their ICT use and digital literacy skills (Livingstone and Bulger, 2013) as well as those of education and health experts.

4.1.2. What do governments do to support children's digital citizenship?

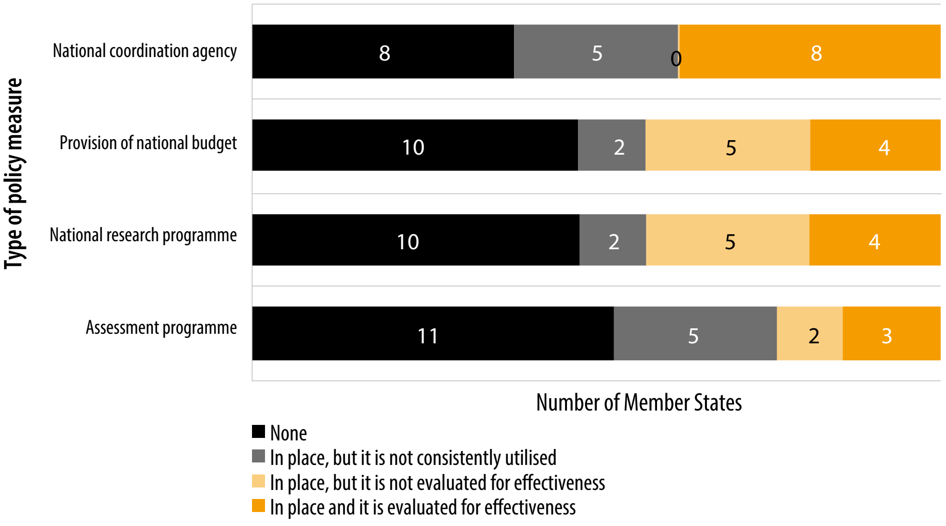
The survey also sought to understand the current efforts and policy measures of governments to support children's digital citizenship, examining: (i) whether a national agency exists to coordinate efforts, (ii) whether the national budget provides for such activities, (iii) whether there is a national research programme and (iv) whether there is an assessment programme in place to measure the efficacy of the digital citizenship policies and programmes.

The responses to the survey indicate that not all of the Member States have all four policy measures in place, but almost half of them have allocated a budget towards supporting digital citizenship in children or have a national coordination agency. The Member States that reported having implemented all four policy measures include Brunei, Malaysia, New Zealand, P.R.China and Singapore.

Over half (57 per cent) of the surveyed Member States reported that they either do not have a national programme to promote the use of research to inform and support policy or, if one is in place, it is not consistently utilised. In these Member States, this would likely lead to policies that are based on assumptions and hypotheses, and that have no evidence of effectiveness rather than policies that are evidence-based.

More than half of the participating Member States reported that they do not have assessment programmes for monitoring and evaluating the efficacy of policies. These are important aspects of policy-making and programme management as introducing such components increases "the likelihood that national ICT education policies and programmes will indeed be implemented" (Kozma, 2008). An overall lack of monitoring and evaluation to measure the effectiveness and efficiency of policies was likewise seen among EU Member States in a study of "Safer Internet" policies (Baudouin, et al., 2014). Figure 4 summarises the responses of the Member States.

Figure 4: Number of Member States that have implemented policy measures to support digital citizenship in children, by type of measure



Note: Japan did not submit responses in this section of the survey.

About four in ten of the Member States surveyed do not have a national agency to coordinate campaigns or activities between the various ministries and departments. However, Singapore's experience, as described in Box 1, has shown that a national coordinating committee or variant of such can benefit Member States' national efforts, including in determining the most up-to-date and relevant themes and issues.

Box 1: Singapore's inter-ministry Cyber Wellness Steering Committee

Singapore's policies on cyber wellness for children are coordinated on a national level by the Inter-Ministry Cyber Wellness Steering Committee (ICSC), which was formed in 2009. The ICSC is co-chaired by the Ministry of Communications and Information and the Ministry of Education and also includes representatives from eight other government ministries and agencies.

The ICSC's aim is to develop and implement a national strategy to promote cyber wellness among youth and equip them through public education to react appropriately to harmful and inappropriate internet content (Media Development Authority, 2015). The ICSC provides funding to support initiatives by the public to further the ICSC's aims and regularly releases calls for proposals to this effect. Its seventh call for proposals, released in December 2015, offered funding for projects that promote cyber wellness in Singapore in areas such as:

- Parenting roles, responsibilities, knowledge and skills for cyber wellness education for children.
- Information literacy, media literacy and responsible online creation.
- Balancing online and offline activities.
- Positive online presence and advocacy for cyber wellness.
- Healthy cyber gaming among children.
- Awareness of gaming addiction and channels of help.
- Awareness of cyber bullying.
- Cyber security and protection against cybercrime.

Between 2009 and 2015, the ICSC funded more than 25 projects, reaching over 245,000 participants (Ministry of Education of Singapore, 2015).

Australia's Children's eSafety Commissioner is a nationally legislated office that coordinates activities to enhance online safety for children (Box 2). This can serve as a good example for other Member States.

Box 2: The Children's eSafety Commissioner

Australia's Office of the Children's eSafety Commissioner is one of the Asia-Pacific region's first examples of a government-legislated and funded office that has the specific mandate of enhancing children's safety online.

Australia established the Office of the Children's eSafety Commissioner in March 2015 as an independent statutory office within the Australian Communications and Media Authority.

The Office of the Commissioner has a wide range of powers and functions as set out under the *Enhancing Online Safety for Children Act 2015,* including promoting online safety for children, coordinating activities between agencies and authorities relating to online safety for children, and administering a complaints system for cyber-bullying material targeted at Australian children. The Office has the power to require social media service providers to take down content.

The website of the Office of the Children's eSafety Commissioner (https://www.esafety.gov.au/) is now a one-stop portal aggregating previously disparate information on all children's cyber safety related initiatives and programmes, and providing resources to children, parents, carers and schools. It also has links to education resources, and online helpline and counselling services such as Kids Helpline.

Monitoring and evaluation is rigorously conducted to ensure continuous improvement and relevance to its target beneficiaries. For example, pre-, immediate, post-, and three-months-post- intervention surveys are conducted among the participants of its national outreach programme, which focuses on the professional development of teachers. Evidence is also gathered on the cost-effectiveness and efficacy of the delivery methods, to feed into the planning process for future cycles.

The Australian government dedicated AUD 10 million in the 2014-2015 budget towards enhancing online safety for children, including AUD 7.5 million to assist schools to access accredited online safety programmes; AUD 2.4 million to establish and operate the Office of the Children's e-Safety Commissioner; and AUD 100,000 to support Australian-based research and information campaigns on online safety (Department of Communications of Australia, 2015).

4.1.3. Are national campaigns conducted on issues relating to children's ICT use?

The survey responses indicate that about 40 per cent of the participating Member States have national campaigns to promote safe and responsible ICT use.

Almost half (about 45 per cent) of the participating Member States develop, implement and/or evaluate campaigns with multiple stakeholder groups to inform communities and stakeholders about the process of reporting ICT abuse and misuse.

Malaysia's national programmes and campaigns provide insight into how national campaigns can raise awareness and reach a great number of children and caregivers in a large country (Box 3).

Box 3: Malaysia's national cyber safety campaigns

Malaysia has two national-level programmes that address cyber safety issues: CyberSAFE and Klik Dengan Bijak ("Click Wisely").

The Cyber Security Awareness for Everyone (CyberSAFE) programme is an initiative by CyberSecurity Malaysia (an agency of the Ministry of Science, Technology and Innovation) that seeks to enhance the awareness of the general public on the technological and social issues facing internet users, particularly regarding the risks they face online. The mission of the CyberSAFE programme is "to impart practical knowledge on cyber safety and provide necessary information and resources to a wide spectrum of the community to ensure their online experience is positive and secure" (CyberSecurity Malaysia, 2016).

Under the CyberSAFE programme is the CyberSAFE in Schools programme, which is a joint effort by a major telecommunications provider, Digi, and CyberSecurity Malaysia, Childline Malaysia, the Malaysian Communications and Multimedia Commission (MCMC) and the Ministry of Education. The CyberSAFE in Schools programme seeks to educate school children in Malaysia on cyber safety and other child welfare issues. It reaches out to school children in Malaysia through various methods, including school outreach programmes using CyberSAFE ambassadors and teacher training workshops.

In 2014, the programme extended its outreach through six pilot workshops at People's Housing Programme communities. It also trained more than 130 ICT teachers, and engaged with 38,000 students and more than 4,100 school teachers (MCMC, 2015). In addition, in 2014, the CyberSAFE in Schools programme conducted an in-depth study that surveyed the internet-related behaviour of almost 14,000 Malaysian school children. The CyberSAFE in Schools programme has produced various books such as the "Guide to Mobile Internet Safety" and has produced videos (available on YouTube) that deal with issues such as cyber-bullying, cyber-stalking and cyber-grooming. The programme also maintains an interactive website on which children can register and learn about cyber safety through contests, games and videos.

The partnership between the government and Digi in the CyberSAFE in Schools programme is a good example of how the public sector can harness the private sector to partner on initiatives to promote a common interest.

Malaysia's other national level programme, Klik Dengan Bijak ("Click Wisely"), which was initiated by the MCMC, is a national public awareness campaign on internet safety. It seeks to cultivate positive internet use, based on safety, vigilance and responsibility.

Emphasizing self-regulation to curb abuse of the internet, the campaign aims to educate internet users about the importance of self-regulation; create a sense of responsibility among internet users so that they behave ethically and are sensitive to others; produce savvy users of technology and new media content; and create a safe environment for internet users. The programme website offers advice on how to deal with issues such as cyber-bullying, pathological gaming and privacy of information. The programme also reaches out to its target audience through booths at multimedia conferences and exhibitions.

Since 2014, under phase two, the campaign has focused on parents and on children aged between 13 and 18. The four main areas of emphasis in this phase are internet addiction, cyber-bullying, dissemination of false information and fraudulent online transactions.

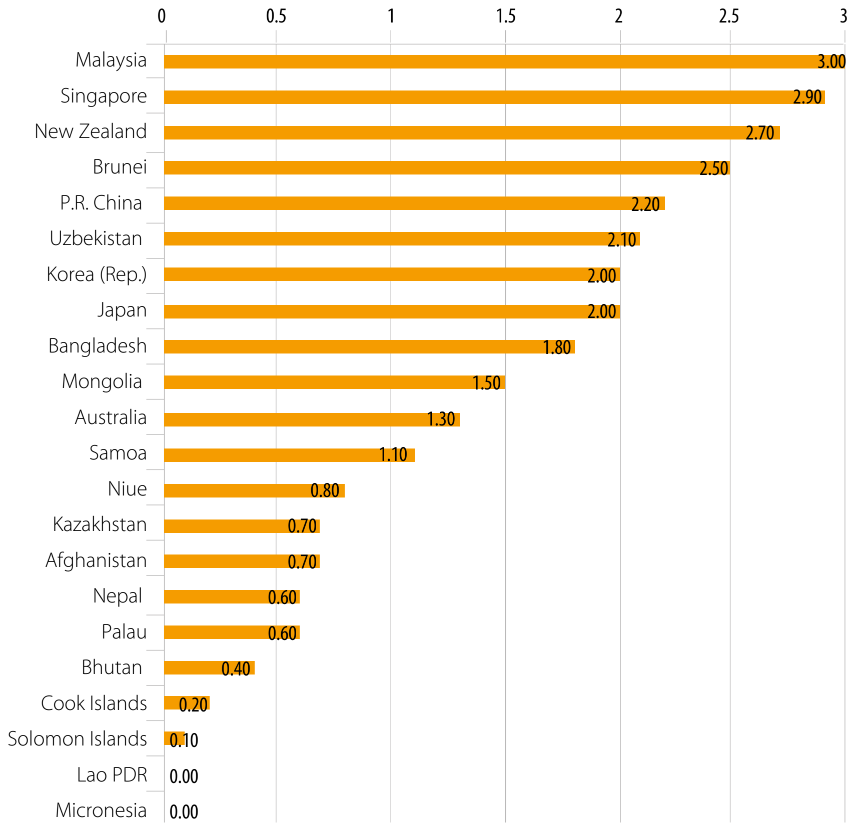
Summary

Overall, the responses to the questions in the Leadership and Accountability category indicate that there is great diversity among Member States regarding their national policies and campaigns. Figure 5 illustrates the policy readiness of the participating Member States for Leadership & Accountability. The level of policy readiness is based on the mean scores of their responses to the survey questions in the Leadership and Accountability category. A score of zero indicates the lowest level in policy readiness (i.e. no policy exists) while a score of three indicates the highest level of policy readiness (i.e. a policy exists, and it is implemented and monitored). The Member States with the highest average scores were Malaysia (3), Singapore (2.9) and New Zealand (2.7).

Linear regression analysis of the variables that predict the level of policy readiness ($r=.929$, $p<.001$) indicates a close link between provisions in the national budget to support digital citizenship policies and the overall level of development of a Member State's policies. That is, those countries with budgets allocated to such policies have highly developed policies.

While most of the countries that have a high level of policy development are high income countries with advanced ICT development, Bangladesh and Uzbekistan are exceptions as they show that a high level of policy development can exist alongside relatively low levels of ICT development and lower income levels.

Figure 5: Overall leadership & accountability policy readiness of participating Member States



Note: Japan did not submit a complete response in this category.

Given the importance of national cyber safety and privacy policies, it is suggested that Member States consider taking a multi-sector approach by involving professionals from all four key sectors: education, health, law enforcement and cyber security in formulating such policies.

Member States can enhance the efficacy of such policies by setting up a dedicated coordination agency, as well as by allocating funding for cyber safety programmes from the national budget, and/or developing a national programme for research and monitoring and evaluation. As the case studies show, several Member States in the Asia-Pacific region have successful ongoing initiatives and programmes related to fostering safe, effective and responsible use of ICT that can serve as models for others.

4.2. Education

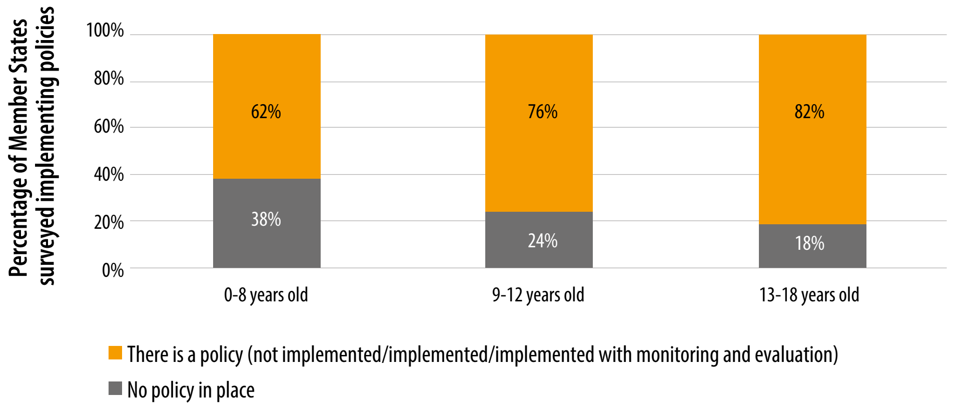
The "Education" category in the survey sets out questions about ICT use and online participation, responsible ethical behaviour, protection against risks, and values reinforcement. Questions in the Education category were divided according to whether they focused on "opportunities" or on "safety and risk". See Appendix 4 for the list of questions belonging to each type.

4.2.1. Are children being taught basic ICT skills in the school curriculum?

Digital citizenship and safe, effective and responsible use of ICT are linked to the possession of basic ICT literacy skills, which allow children to explore the online environment and take advantage of the communication, learning and social aspects of ICT. Children across the Asia-Pacific region vary in their level of ICT literacy, due to the differences between the Member States in economic development levels and the resources dedicated to ICT for formal education. While ICT is ubiquitous in high-income countries in the Asia-Pacific region, the integration and use of ICT in education – especially more advanced forms of ICT– is often limited in many developing countries. Consequently, children and youth in developing countries tend to "learn more about how to use ICT informally outside of the school system than in the classroom" (UNESCO Institute for Statistics, 2014, p. 11).

The survey responses indicate that most of the participating Member States are already encouraging students of all age groups to learn basic ICT literacy skills. Nearly all (over 80 per cent) of the surveyed Member States have national policies, programmes and resources targeting secondary school students (aged 13 to 18) that promote basic ICT literacy skills, although these policies and initiatives vary in their degree of readiness (Figure 6).

Figure 6: Percentage of Member States that promote basic ICT literacy skills in children, by children's age groups.



These responses suggest that most Member States in the region understand the importance of digital literacy and agree that "early integration of ICT into primary and secondary curricula … is vital" (UNESCO Institute for Statistics, 2014, p. 11).

4.2.2. Are children being empowered to be active participants in the digital world?

Researchers suggest that children climb a "ladder of opportunities" for internet use by seeking out information, using games and communication tools and later creating content and engaging in interactive use (Livingston and Helsper, 2007). As the digital world evolves, these different opportunities may merge and no longer be separate activities. One example of this is "Web 2.0", wherein multiple modes of communication and information sharing are integrated. One aspect of the Web 2.0 is social networking sites (SNS), which integrate chat, messaging, contacts, photo albums and blogging functions, thereby integrating online opportunities and risks more seamlessly than previously (Livingstone et al., 2011).

Research shows that many children in Europe and Australia have their own SNS profiles. In 2011, around two thirds (65 per cent) of Australian children aged 9-16 reported having an SNS profile, while more than half of the children aged 11-12 and 29 per cent of children aged 9-10 said they had one (Green, et al., 2011). This is in spite of the rules of SNS companies, such as Facebook, that require users to be a minimum of 13 years old. A similar survey in Indonesia found that 63 per cent of children aged 10-18 access SNS and micro-blogging sites on their mobile phones, while a survey in Japan found that 44 per cent of this age group access such sites on their phones (Groupe Spéciale Mobile Association, 2013). These figures indicate that the current usage of SNS by children is high in the Asia-Pacific region.

The survey results show that over half (55 per cent) of the surveyed Member States have implemented policies that aim to empower children aged 13-18 with more sophisticated, creative and participatory ICT skills to conduct online research, communicate, create content, and view and share content through safe and responsible social networking. The figures were lower for younger age groups, namely 43 per cent for the 9-12 age bracket and 38 per cent for children under 9.

Given the current trends for ICT use by children, including SNS, the survey responses indicate that in almost half of the surveyed Member States education policies are lagging behind the trends. It may be necessary to implement policies targeting all children, not just older children, as research suggests that the age of 11-12 is a "tipping point" for a significant increase in the use by children of SNS and other social media (Green et al., 2011) and interventions are required before this age.

4.2.3. Is national policy addressing the trend of children using personal ICT devices?

Research in the Asia-Pacific region has found that an increasing number of children across all ages are using mobile phones and other ICT devices, and children are accessing the internet at younger ages than in the past (Groupe Spéciale Mobile Association, 2013; TheAsianParent Insights, 2014; Green et al., 2011; NZ On Air, 2015). If Member States fail to implement policies to capitalize on children's patterns of use, it could be a missed opportunity to leverage upon the use of ICT in the classroom.

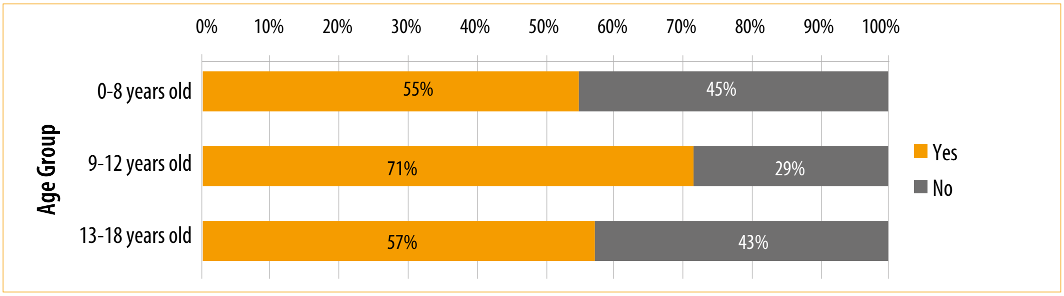
In this context, it is of concern that more than half of the surveyed Member States have no policies to promote the use of student-owned devices in schools or have not implemented such policies. Almost two-thirds of the surveyed Member States (62 per cent) do not have such policies or do not implement them for children aged 0-8 and 13-18 and 57 per cent do not have such policies or do not implement them for children aged 9-12.

4.2.4. Are teachers being supported to be active advocates for cyber wellness?

The lack of knowledge and skills in ICT among teachers has been identified by researchers as one of the major obstacles to the use of computers in schools. Researchers suggest that teacher training programmes play an important role in providing pre-service and in-service teachers with the required skills (Afshari et al., 2009). To ensure teachers have the necessary capacity to integrate ICT into education, Member States need appropriate policies regarding pre-service and in-service teacher training programmes.

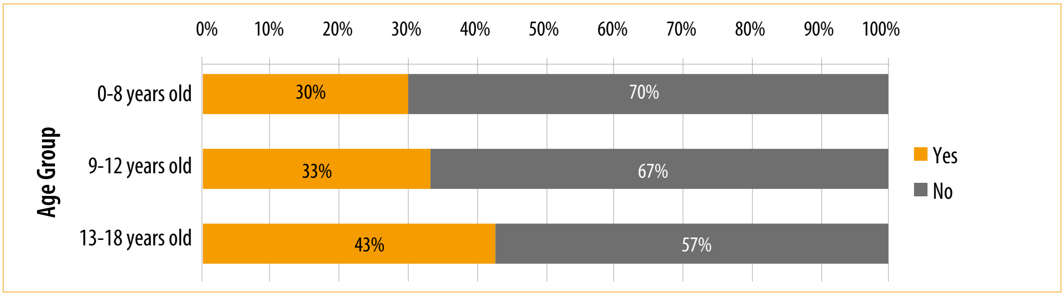
Appropriate policies for in-service teachers and school staff are implemented in the majority of Member States, with survey participants reporting that they having implemented teacher training programmes on the use of ICT in schools. In particular, 71 per cent of Member States implement such policies at the primary school level, 57 per cent at the secondary school level and 55 per cent at the early childhood and early primary level (Figure 7).

Figure 7: Percentage of Member States that implement policies to promote training for teachers in the use of ICT in school



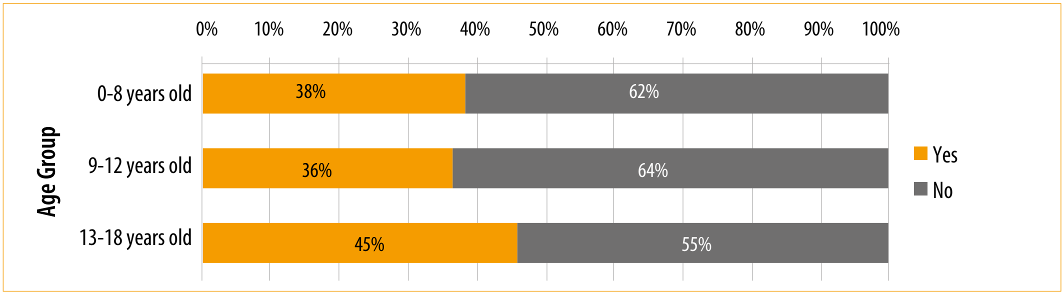
However, the survey responses indicate that only between 30 per cent and 43 per cent of the Member States surveyed have incorporated national standards on ICT literacy skills, cyber wellness and cyber security skills into teacher preparation programmes, as illustrated in Figure 8.

Figure 8: Percentage of Member States that implement policies to promote national standards for teacher preparation that include ICT literacy skills, cyber wellness and cyber security skills



The responses also indicate that, as with students, the participating Member States tend to prioritize imparting basic ICT skills to teachers over more advanced skills. Only between 36 per cent and 45 per cent (measured across the three age groups) have implemented programmes that provide teachers with more advanced skills, such as ICT-pedagogy competencies, digital citizenship and cyber wellness education (Figure 9).

Figure 9: Percentage of Member States implementing policies that promote programmes for in-service teachers on ICT use in education that include cyber wellness and cyber security components



On average, 45 per cent of participating Member States implement policies to support the development of teachers' ICT skills and cyber wellness and cyber security competencies. Thus, the responses indicate that there is a distinctly better implementation rate for policies relating to training of teachers in the basic use of ICT than for more advanced ICT skills, digital citizenship and cyber wellness competencies.

The survey responses suggest that although the surveyed Member States understand the importance of gaining basic ICT literacy skills in the formal education system, many Member States have policy gaps when it comes to policies to address the needs of the various audiences i.e. students and teachers. Considering that a "lack of professional development for technology use is one of the most serious obstacles to fully integrating technology into the curriculum" (Afshari et al., 2009), the responses show that there is room for improvement in the implementation of such policies.

It is suggested that Member States attempt to bridge the gaps in the implementation of policies by establishing national standards or similar national-level mechanisms to ensure that teachers are better supported and equipped to teach cyber wellness and security effectively.

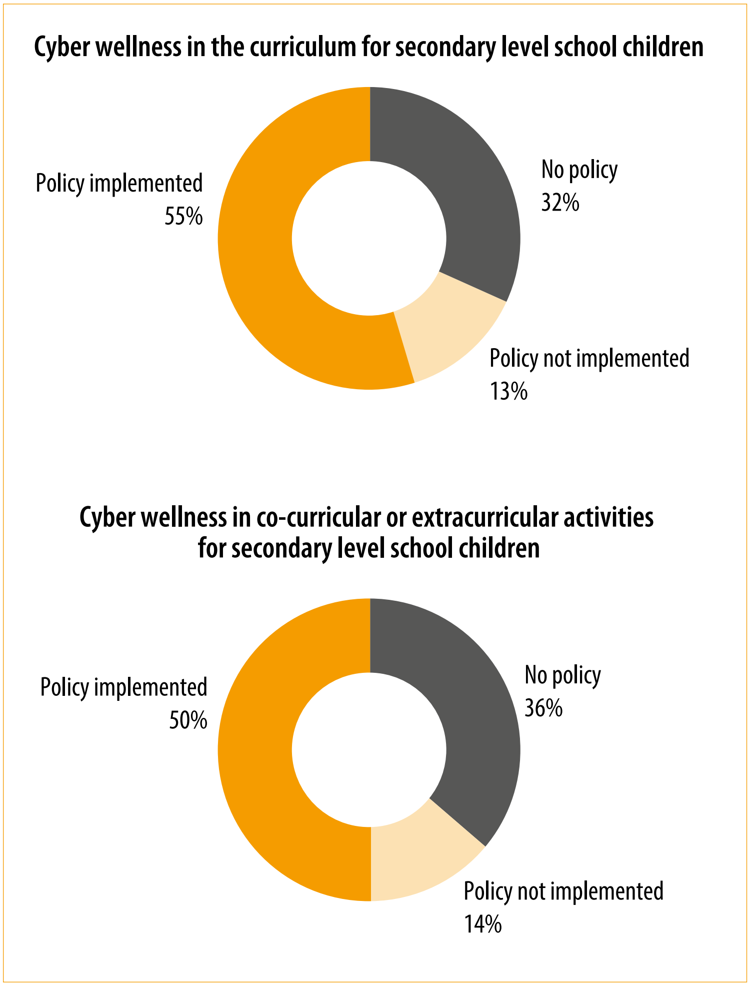
4.2.5. Is the school curriculum promoting cyber wellness?

The survey also asks whether policies existed to encourage schools to explicitly promote the safe and responsible use of ICT and cyber wellness. According to the responses, between 50 per cent and 60 per cent of the Member States do not implement policies integrating the promotion of the safe and responsible use of ICT and cyber wellness into the curriculum or into co-curricular/extracurricular activities in schools for the early childhood and primary school age groups.

The responses to the surveys indicate that while the surveyed Member States have policies in place regarding the promotion of basic ICT literacy skills among children of all age groups, not all Member States have such policies in place for the development of higher-order ICT skills such as cyber security skills and competencies. Only around half of the surveyed Member States have policies in place for teaching such skills to children aged 0-8 years old, while over half of the Member States have such policies for children aged 9-12 years old. Even at the secondary school level, only around half of the Member States implement policies to integrate the safe and responsible use of ICT into the curriculum or into co-curricular or extracurricular activities (Figure 10).

Research in Europe indicates that policy-makers anticipate that the more digitally-literate or skilled children become, the more they will gain from the internet and the better-prepared they will be to avoid or cope with online risks (Livingstone et al., 2011). To maximise the potential of children to take advantage of the opportunities afforded by ICT and the internet, Member States should consider implementing policies that also address advanced ICT skills.

Figure 10: Percentage of Member States implementing policies targeting individual schools that promote cyber wellness in the curriculum and in co- or extra-curricular activities for secondary school children



Singapore's Cyber Wellness Framework is an example of an outcome of balanced policies being implemented within the formal education system and applied across all schools as part of the curriculum for children aged 7 to 18 (Box 4).

Box 4: Singapore's Cyber Wellness Framework

"Cyber wellness" refers to the well-being of internet users. It involves having an understanding of the norms of appropriate, responsible behaviour with regard to mobile and technology internet use as well as the knowledge, skills, values and attitudes on how to protect oneself and other internet users, avoid dangers online and evaluate the consequences of one's choices. It seeks the positive physical and psychosocial well-being of students in their use of mobile and internet technologies (Ministry of Education of Singapore, 2014).

A major aspect of the national strategy for cyber wellness education in Singapore is the Ministry of Education's Cyber Wellness Framework, which became compulsory in 2014 for students in the public school system aged 7-18. The Cyber Wellness curriculum "aims to equip students with lifelong social-emotional competencies and sound values so that they can become safe, respectful and responsible users of ICT" (Ministry of Education of Singapore, 2016).

Prior to 2014, schools were guided by a Cyber Wellness Framework set out by the MoOE to plan and implement programmes that were customised to their student profile and school environment. Since 2014, as part of the Character and Citizenship Education curriculum, secondary schools are required to dedicate four hours of curriculum time to the delivery of cyber wellness lessons for each academic level. At primary school level, the cyber wellness syllabus is integrated into Character and Citizenship Education lessons conducted by the teachers.

Highlights of the Cyber Wellness Framework:

Two principles: Respect for self and others, and safe and responsible use of ICT.

Three Big Ideas: Identity, relationships, choices.

Four themes: Cyber identity, cyber use, cyber relationships, cyber citizenship.

Eight topics: Online identity and expression, balanced use of ICT, netiquette, cyber-bullying, online relationships, about the cyber world, handling content behaviour, cyber contacts.

Figure 11: Cyber Wellness Curriculum (Singapore)

2 Principles - 3 Big Ideas - 4 Themes

2 Principles	3 Big Ideas	4 Themes	8 Topics
SENSE CYBERWELLNESS PRINCIPLES • Respect for Self and Others • Safe and Responsible Use ACT THINK • Respect for self and others • Safe and reponsible use	Identity	• Cyber igentity: Healthy self-identity • Cyber Use: Balanced life and balanced use	• Online identity and Expression • Balanced Use of ICT
	Relationship	• Cyber Relationships: Safe and meaningful	• Netiquette • Cyber Bullying • Online Relationships
	Choices	• Cyber Citizenship: Positive presence	• About the Cyber World • Handling Online Content and Behaviour • Cyber Contacts

Source: Ministry of Education – Singapore.

As part of the programme's multi-stakeholder approach, parents are recognized as being essential to ensuring better uptake of cyber wellness principles by students. For example, the secondary school cyber wellness syllabus suggests that teachers advise parents on setting boundaries on internet use and being good examples to their children to reinforce cyber wellness principles learned at school, and that workshops be conducted for parents to increase their knowledge. Also, the syllabus recommends the recruitment of external agencies (outside of MOE), such as the Health Promotion Board and the Media Development Authority, to conduct information sessions with students, teachers and parents.

Educating the wider community on the safe, effective and responsible use of ICT is another policy that would support the creation of a safe environment for children's interactions with ICT. Policies that promote educational sessions on safe and responsible use of ICT and cyber wellness among caregivers would create such environments. It is therefore alarming that only an average of 35 per cent (across all the age groups) of the participating Member States implement such a policy that promotes educating caregivers.

The lack of policies and implementation in this regard limit the opportunities for children to engage with caregivers, teachers and school leaders about issues arising from ICT use and cyber wellness. These avenues, within the curriculum and through co-curricular and extracurricular activities, offer a two-way engagement in a safe environment to discuss both *risks* such as cyber bullying, exposure to disturbing content and meeting people online and *opportunities* such as content creation, participating in online communities, and developing ICT skills and competencies.

Research in Australia found that 83 per cent of children aged 9 to 16 years old receive their first internet safety advice from teachers (Green et al., 2011). While the context and culture of each Member State is different, the findings suggest that more can be done in schools to maximize the time children spend receiving advice and acquiring skills relating to the safe and responsible use of ICT.

Attempts to maximize awareness both in schools and in communities are particularly important because the use of personal ICT devices among children is becoming more and more common. Australia has several programmes and initiatives that take a broad-based, community-wide approach to cyber safety education and serve as useful examples (Box 5).

Box 5: Australia's programmes and initiatives to educate the wider community

Australia has a wide range of programmes and initiatives to promote digital citizenship and cyber-safety education in children at both the federal and state government levels. These include the following:

- ThinkUKnow

The Australian Federal Police partnered with the state and territory police forces and with industry partners in 2009 to launch the ThinkUKnow programme, which "is a free, evidence-based cyber-safety programme that provides accessible cyber-safety education to children, parents, carers and teachers through schools and organizations throughout Australia" (ThinkUKnow website). An important part of its message is that children, parents, carers and teachers should learn about ways of using technology positively and not simply be concerned about the potential misuse and risks that may occur. The programme conveys its message through free face-to-face and digitally-delivered sessions run by law enforcement volunteers and industry partners. Information and resources are also available through its website.

- Stay Smart Online

The Department of Communications and the Arts hosts the Stay Smart Online website, which aims to assist the public to understand the risks of the online environment and the steps they can take to protect their information online. The website contains resources for parents and teachers on the range of issues that children might face online. The website also provides information specifically for children regarding using social media safely.

- National Safe Schools Framework

The Department of Education and Training works closely with the Department of Communications and the Arts on the issue of cyber-safety in schools, aiming to ensure evidence-based cyber-safety education is available to all school communities. The Department of Education's National Safe Schools Framework, supported by the online resources of the Safe Schools Hub, assists school communities in building a positive school culture and tackling issues such as bullying and cyber-bullying. The Department of Education provides links to resources such as the Cybersmart Programme, now administered by the Office of the Children's eSafety Commissioner, and the 'Bullying No Way!' educational website to prevent bullying, including cyber-bullying, in schools.

4.2.6. Are adults assisted in becoming mediators of children's ICT use?

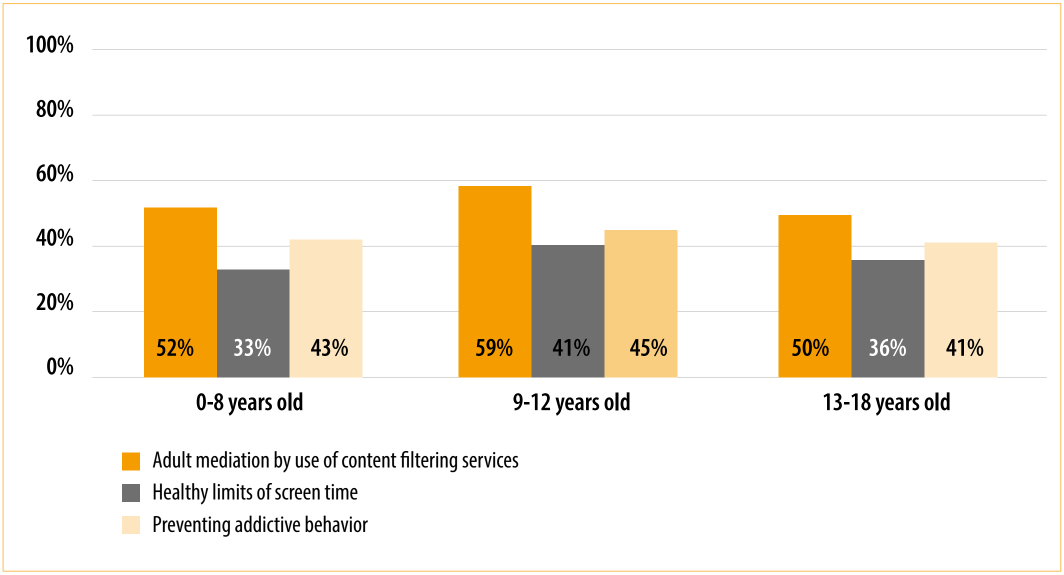
The survey asks three questions about whether the ministries of education had policies targeting adult caregivers (parents, guardians and teachers) in promoting adult mediation of ICT use in three areas: content filtering to prevent access to inappropriate content; healthy limits on screen time; and preventing or reducing conduct relating to pornography, gaming and other addictive behaviour.

Four of the Member States reported having implemented all three types of policies and across all three age groups. These Member States were Brunei, Japan, Malaysia and P.R. China.

On average, 42 per cent of the surveyed Member States have implemented one or more types of policies promoting appropriate adult mediation in the three areas among secondary school children aged 13-18, while almost half of the surveyed Member States have implemented such policies for children aged 9-12 and 43 per cent for children aged 0-8.

The most common type of policy reported by the Member States was the use of content filtering services. About half of the participating Member States have implemented that type of policy for children aged 0-8 and 13-18 years old. Even more (59 per cent) have done so for children aged 9-12 (Figure 12).

Figure 12: Percentage of Member States implementing policies related to appropriate adult mediation of children's ICT use, by type of policy and age group



The school is a potential avenue for engagement with children on prevention and intervention regarding access to pornography, gaming and other addictive behaviour. However, about 45 per cent of the Member States surveyed do not have policies in place in this regard.

4.2.7. Are policies balanced in promoting opportunities and preventing risks?

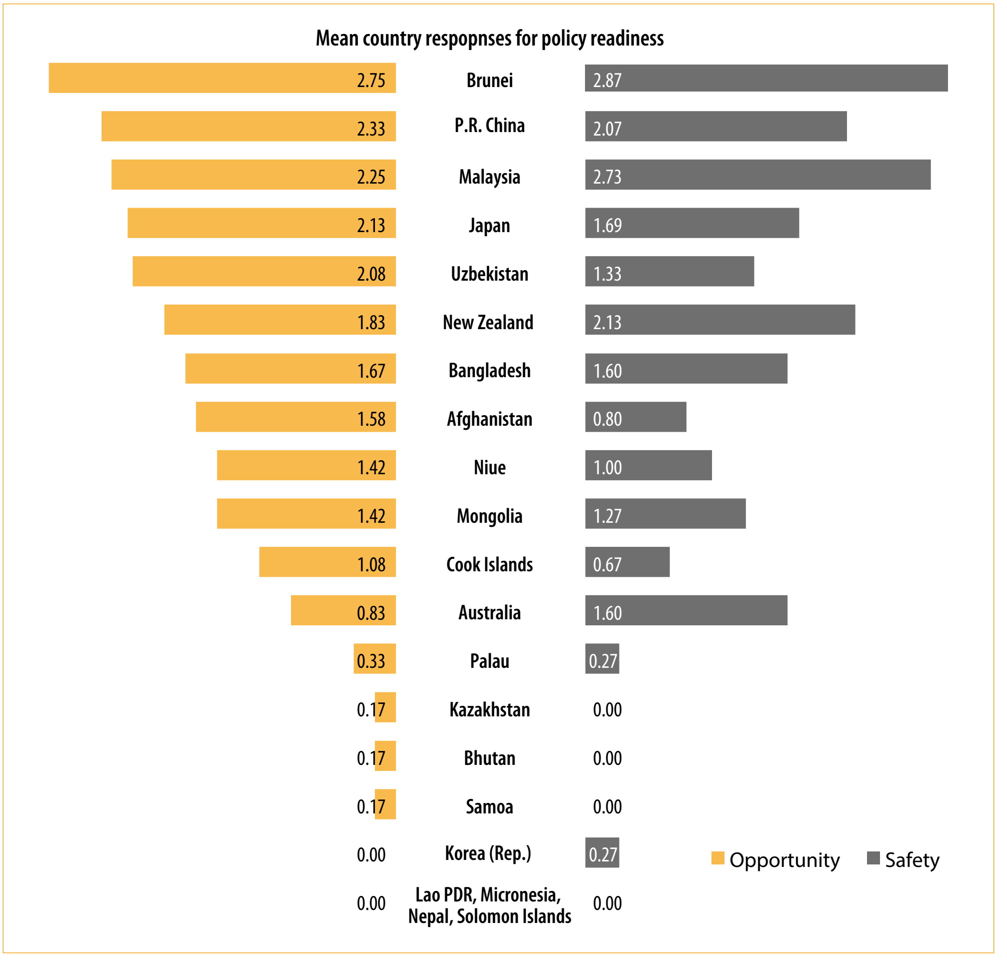
One of the main goals of UNESCO's "Fostering Digital Citizenship through Safe, Effective and Responsible Use of ICT" project, under which the policy review was conducted, is to increase awareness and promote the opportunities of ICT use by children while simultaneously mitigating accompanying risks. The project seeks to encourage balanced policies, whereby the opportunities offered by ICT are made available to children while risks are minimized and safety is increased for children in their interactions with ICT.

Opportunity-oriented policies are those that promote ICT access and use, and the creation of ICT-enabled outputs. Facets of opportunity that were examined in the survey included digital storytelling; computer coding; production of ICT-enabled outputs; creating, communicating and collaborating online; and the use and publication of digital and video images. The survey also asked about policies that target educators and caregivers, e.g. training teachers in ICT literacy and on the use of ICT in school, which affect the quality of students' learning of ICT skills and access to the online environment.

Policies that are oriented towards safety and risk include those that seek to ensure students have the necessary skills to protect their privacy and that ensure cyber security. The survey examined school-level policies that encourage schools to adopt "acceptable use policies" in relation to ICT use and to ensure students learn about safe and responsible use of ICT and cyber wellness through incorporating these into the curriculum and into co-curricular and/or extra-curricular activities. The survey also examined whether the Member States have policies that aim to ensure caregivers engage in appropriate adult mediation for children's ICT use, through guidance on privacy of information and data security; content filtering; and prevention of access to pornography and online gaming.

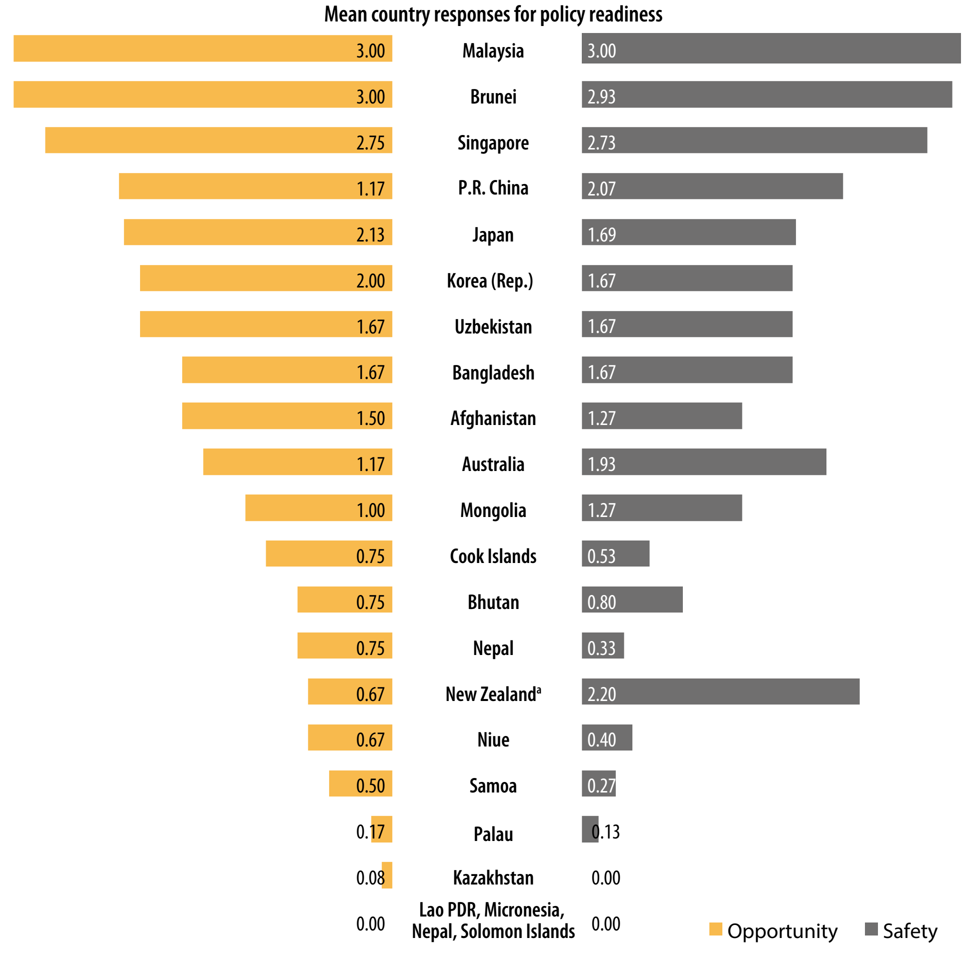
For the early childhood and early primary age group (children aged 0-8), the survey responses indicate that in Malaysia, New Zealand and Australia, the policies relating to safety and risk are emphasised more compared to those relating to opportunity. In contrast, Member States such as P.R. China, Japan, Uzbekistan, Cook Islands and Niue have significantly more opportunity-oriented policies than those oriented to safety and risk (Figure 13). This finding indicates that there is a wide variety of policy environments among the Member States for this age group. Despite this, survey results for pre-primary age group show a strong positive correlation (r = 0.926) between policy readiness to promote opportunities and policy readiness to prevent risks.

Figure 13: Mean scores of Member States regarding policies oriented towards opportunity vs those for safety and risk (children aged 0-8)



For children aged 9-12, the Cook Islands, Japan, Korea (Rep.) and Uzbekistan have more emphasis on opportunity-oriented policies compared with those relating to safety and risk. The survey responses indicate that New Zealand has significantly more policies oriented to safety and risk than opportunity-oriented policies, but this is likely to be due to an incomplete response in this age group (Figure 14). Nevertheless, survey results reveal a strong and positive correlation (r = 0.915) between a Member State's policy readiness to empower children to embrace ICT opportunities and policy readiness to address related risks among children aged 9-12.

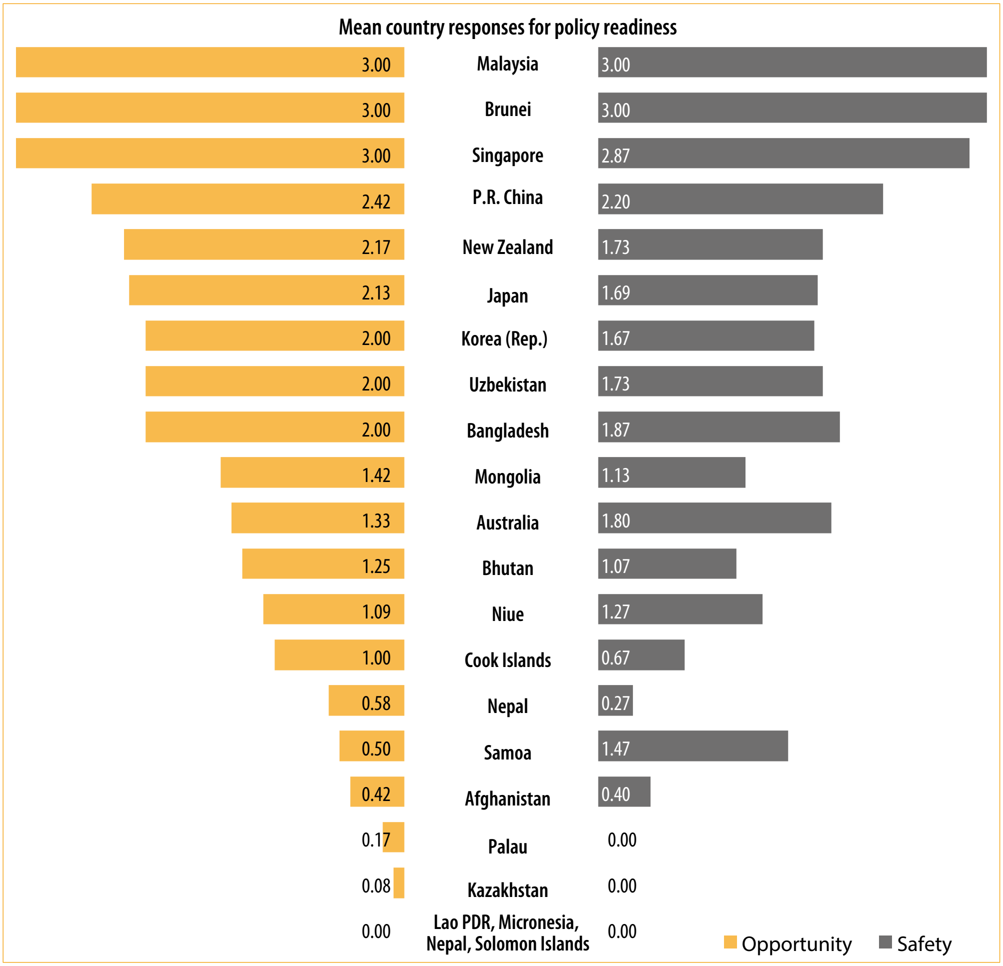
Figure 14: Mean scores of Member States regarding policies oriented towards opportunity vs those for safety and risk (children aged 9-12)



[a] Incomplete response in this age group

For children aged 13-18, the responses of the surveyed Member States indicate that most Member States have more emphasis on opportunity-oriented policies compared to risk-oriented policies, particularly the Cook Islands, Japan, Niue, P.R. China, Korea (Rep.) and Uzbekistan. On the contrary, Australia, Samoa and Afghanistan have more policies oriented to safety and risk than to opportunity (Figure 15). Consistent with the findings for the other two age groups, for children aged 13-18, Member States' policy readiness to embrace ICT opportunities were found to have a strong and positive correlation (r = 0.979) with their policy readiness to prevent related risks.

Figure 15: Mean scores of Member States regarding policies oriented towards opportunity vs those for safety and risk (children aged 13-18)



Overall, the findings imply a positive picture. With only a few exceptions, the analysis indicates that participating Member States have a balanced approach that encourage ICT opportunities as well as emphasize safety and minimise risks. That is, in general, countries set up measures for digital safety alongside those that encourage digital opportunities.

Figure 16 compares to what extent each Member State implements opportunity-oriented policies across the three age levels. It illustrates that across the surveyed Member States, opportunity-oriented policies focus more on children aged 13-18 than on children aged 0-12, with a few exceptions like Uzbekistan, Australia, Nepal and Afghanistan where the focus is given to children aged 9-12. The findings are similar for policies oriented towards safety and risks, with more of these policies targeting children aged 13-18 (48.3 per cent) than targeting children aged 9-12 (44.7 per cent) and aged 0-8 (37.7 per cent). There are not only fewer policies for the younger age groups but there is also a lower rate of policy implementation (Figure 17).

Figure 16: Mean scores of Member States for opportunity-oriented policies, by age group

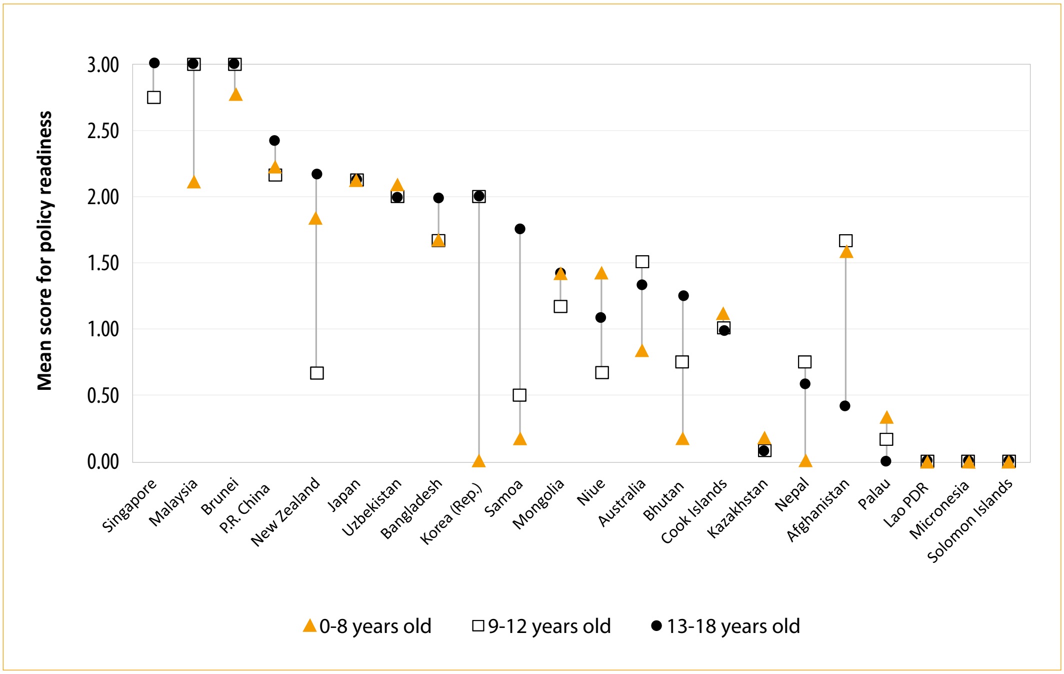
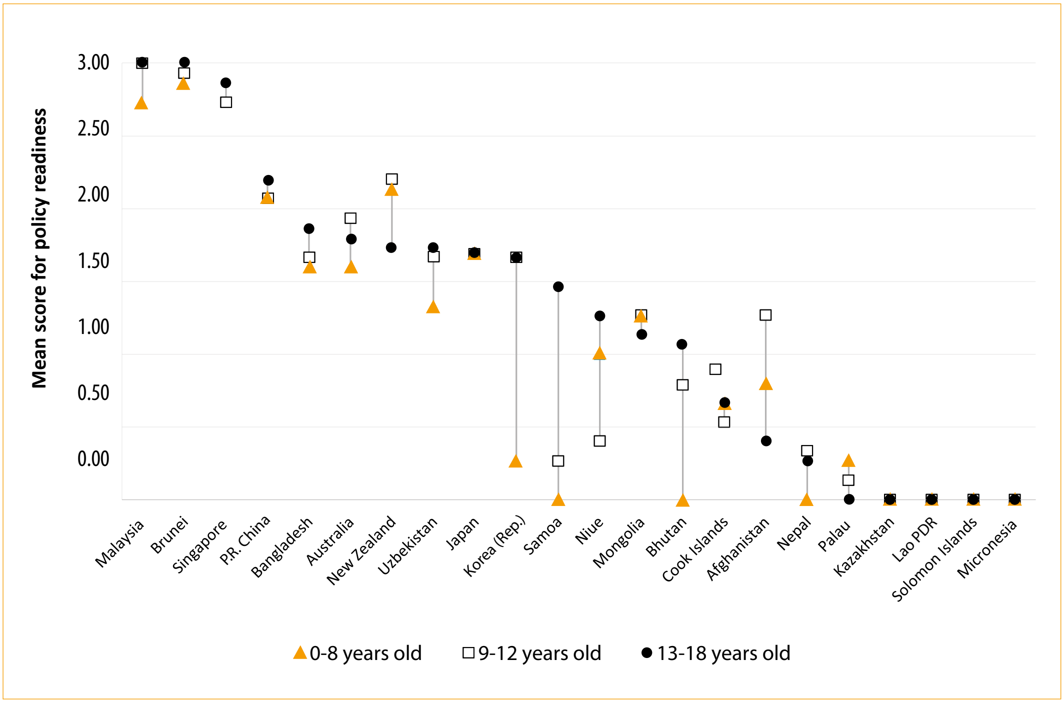


Figure 17: Mean scores of Member States for policies oriented to safety and risk, by age group



The priority placed on the older age groups is a cause for concern as research in both neuroscience and social science have repeatedly found that it is in early childhood "that genetic potential interacts in infinitely complex ways with early experience to construct the neural pathways and connections that quickly become both the foundations and the scaffolding for all later development" (UNICEF, 2013). Young children are particularly vulnerable when interacting with ICT because they have little awareness of what the "internet is, what 'online' means, what risks they can encounter or the benefits they can gain" (Chaudron, 2015).

In addition, governments should consider the benefits of public-private partnerships as a complementary and effective means of imparting advanced ICT skills to children. The case of Intel in India is a successful example of such public-private partnership (Box 6).

Box 6: Intel India's Digital Wellness programme

As part of Intel's efforts in India to promote awareness among children and youth of the benefits and risks of online activities, Intel has conducted several awareness campaigns for students. It has also participated in the development of a Digital Wellness curriculum and created a set of guidelines for ICT practices with cyber safety regulations.

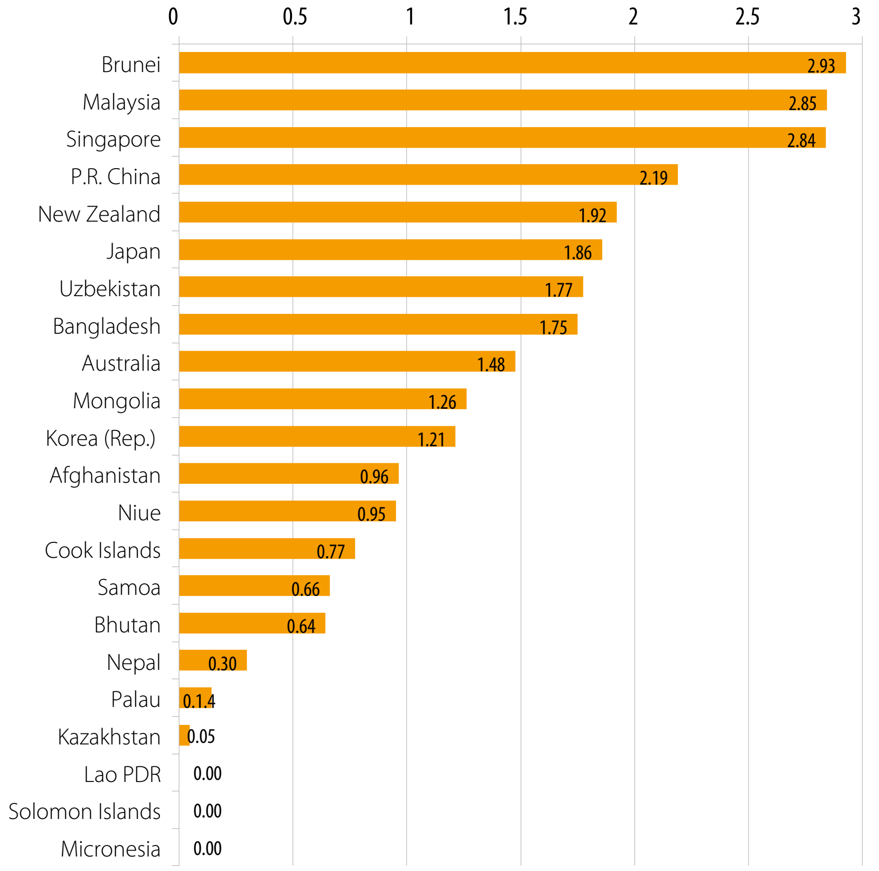
The Digital Wellness curriculum engaged school children aged 13-18 in various activities that aimed to build their understanding of both the benefits and dangers of online activities and to enable them to make responsible and informed decisions, especially on social media platforms.

In July 2015, Intel collaborated with the National e-Governance Division of India's Ministry of Communications and Information Technology to organize a Digital Wellness Online Challenge as part of Digital India Week. Students were asked to complete a series of questions based on their knowledge of digital wellness and decision-making within cyberspace. The challenge had almost 1 million participants, with 144 winners from across 36 states. The winners were invited to participate in a national event and met with top officials from the Ministry of Communications and Information Technology.

Summary

Figure 18 shows the overall policy readiness of the participating Member States in providing education environments where children's safe, effective and responsible use of ICT is actively encouraged and promoted. The level of policy readiness is based on the mean score of the survey questions in the Education category. Brunei (2.93), Malaysia (2.85), and Singapore (2.84) score the highest in this category, indicating that they have comprehensive policies, which are also being implemented. Bangladesh (1.75) and Uzbekistan (1.77) stand out for their relatively high policy scores considering their lower levels of internet development and financial resources compared to similarly scored peers.

Figure 18: Overall education policy readiness of participating Member States



Note:

Singapore was unable to submit responses to 28 questions in the 0-8 years old age group.
Japan was unable submit responses to 19 questions across all three age groups.
New Zealand was unable to submit responses to 20 questions in the 9-12 years old age group.
Brunei and Samoa were unable to submit a response to one question in the 13-18 years old age group.

The findings in the education category of the survey show several key characteristics of Member States' education policies regarding children's ICT use and the safe and responsible use of ICT. These characteristics are summarized below.

- A lack of policies for children in the early childhood and early primary age group of 0-8 years old.

  This applies to both opportunity-oriented policies and safety- and risk-oriented policies and many policies in general. This finding also resonates with international concerns regarding the lack of treatment to this aspect of education (Sefton-Green, Marsh, Erstad, & Flewitt, 2016). While Member States may not be in a position to implement policies at present, the findings raise a pressing concern as early childhood development sets the foundation and scaffold for all later development.

- A focus on basic ICT skills.

  While Member States have generally recognized and taken steps to educate children on basic ICT literacy skills in the formal education system, additional policies on higher-order ICT skills such as content creation, cyber security skills and privacy skills could be developed and implemented to better equip children to become active digital citizens.

- Insufficient development of teachers' ICT skills.

  To complement the development of children's ICT literacy skills and higher-order ICT skills, Member States can better support the development of teachers' ICT skills, cyber wellness and cyber security competencies. Notably, there is a distinctly better implementation rate of policies for the training of teachers on the use of ICT provisions in schools, which could be attributed to a focus on imparting basic ICT skills over higher order ICT-pedagogy competencies or digital citizenship and cyber wellness education.

- Member States generally have balanced policies.

  Across the three age groups surveyed, opportunity-oriented policies are shown to be strongly and positively correlated ($r > 0.9$) to risk-prevention policies. This is a positive finding as researchers recommend that policies should not be overly focused on the perceived risks to children of ICT use. This sets the stage for further research into the realities in the Asia-Pacific region regarding the actual ICT opportunities being taken up by children versus the risks children face.

4.3. Technical Infrastructure

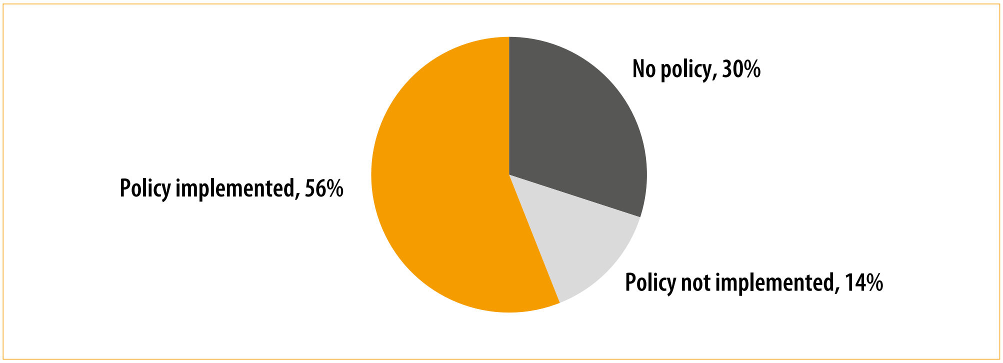
Technical infrastructure is relevant to the issues of digital citizenship and cyber well-being of children in two ways: by enabling children to access and use computers and other ICT tools and the various online opportunities that facilitate the development of digital literacy skills; and by ensuring the security and privacy of children's data within formal education systems.

4.3.1. Are Member States providing children with basic ICT infrastructure?

The responses to the survey indicate that most of the participating Member States recognize the importance of providing ICT infrastructure in schools. According to the responses, the ministries for education in about 75 per cent of surveyed Member States have policies promoting basic ICT literacy skills in children and also have policies to provide at least one computer lab per secondary school.

Across the three age groups, an average of 56 per cent of the surveyed Member States have a policy promoting a minimum of one computer lab per school and have implemented that policy (Figure 19). On average, 14 per cent of the surveyed Member States have such a policy but have not implemented it, indicating that some Member States have difficulties implementing their policies at the school level.

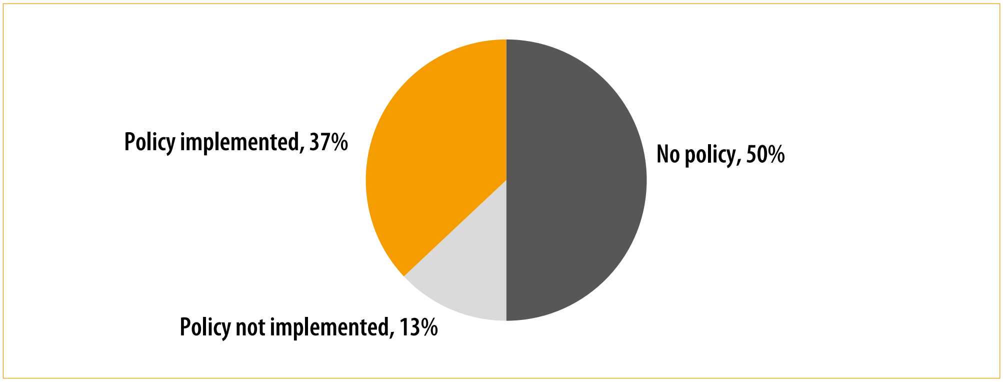
Figure 19: Percentages of Member States that promote the provision of at least one computer lab per school in their policy (across all age groups)



Implementing a national policy that ensures a minimum bandwidth in schools would improve the quality of internet access in schools. This should increase the use of the internet by children in schools, which studies predict would assist them to take up more online opportunities and become more digitally literate (Livingstone and Helsper, 2010). If schools in the Asia-Pacific region are not adequately exposing children to the online environment, which forms a large part of ICT opportunities, this will impede their ability to gain and/or deepen ICT literacy skills and digital citizenship competencies.

The survey responses indicate that half of the surveyed Member States do not have a policy in place to ensure a national level at which schools' minimum bandwidth requirements must be set. The other half of the Member States have such a policy, but only about one-third of these Member States actually implement it (Figure 20).

Figure 20: **Percentages of Member States that promote setting a minimum bandwidth for schools in their policy (across all age groups)**



When analysed by age group, the findings show that the surveyed Member States' ICT infrastructure policies focus more on secondary school children than on primary and early primary children. While 66 per cent of the surveyed Member States have at least one computer lab per school for children aged 13-18, fewer (57 per cent) have the same for children aged 9-12 and only about 45 per cent have the same for children aged 0-8.

Similarly, in the case of policies relating to schools' minimum bandwidth, 45 per cent of the surveyed Member States have implemented such policies for secondary school children, whereas fewer (40 per cent) have done so for primary school level children and only 25 per cent have done so for the youngest children (aged 0-8).

While it may not be possible to provide equal levels of ICT infrastructure for all age groups, it is possible for most countries to provide at least some level of ICT infrastructure for each age group. Kazakhstan's national policy for ICT in education provides an example of a Member State's successful efforts to improve technical infrastructure at all levels of education (Box 7).

Box 7: Kazakhstan's policies to improve its technical infrastructure

Kazakhstan has a very strong focus on education as part of the main priorities of the "Kazakhstan 2030" strategy. The education reforms outlined in the strategy aim to adapt the education system to the new socio-economic environment. This aim is aligned to the overall goal set by the President of Kazakhstan for the country to become one of the 50 most competitive countries in the world.

Kazakhstan's national policy for ICT in Education is part of the "State Programme of Education Development for 2011-2020" (SPED). The goal of the SPED is to develop human capital by ensuring access to quality education. ICT is viewed as an essential aspect of education as it is vital in ensuring that human capital have the skills and abilities to succeed in the workplace.

The SPED ICT in Education policy focuses on e-learning as a means to ensure equal access for all to education resources and technologies. The key components of the SPED e-learning policy are as follows:

- Develop technological infrastructure to provide for the connection of educational institutions to the internet with the capacity of 4-10 megabytes (MB) per second.
- Upgrade teachers' qualifications in the use of e-learning systems.
- Connect over 90 per cent of educational institutions to the internet, particularly the schools that are part of the resource centre pilot projects.
- Ensure 90 per cent of education organizations have internet-resources and necessary academic resources.
- Ensure interactive and intellectual digital academic resources are developed for each subject studied at secondary and profession-oriented schools.
- Establish an arrangement by which school students keep personal portfolios, calendars and diaries in a computerized system. The teachers will fill in electronic notebooks with calendar-thematic planning, class journals and alerting services (sending e-mails or SMS to parents about upcoming meetings and appointments, reporting data, etc.).
- By 2015, ensure that 50 per cent of education institutions are using e-learning at all levels of training. And 90 per cent of institutions by 2020. Pre-school education institutions will use computer programmes and computerized educational games.

4.3.2. Are school networks secure?

In general, schools in the surveyed Member States lack secure ICT networks. This results in a lack of protection for the transmission of data and for data on school-based ICT systems. On average, slightly more than one third of the surveyed Member States have implemented policies addressing issues of security and privacy of data in school-based ICT systems (Table 4). Thus, the survey responses indicate that schools in almost two thirds of the surveyed Member States are vulnerable to malicious activities that could access children's personal information stored on those systems.

Table 4: Security of school networks

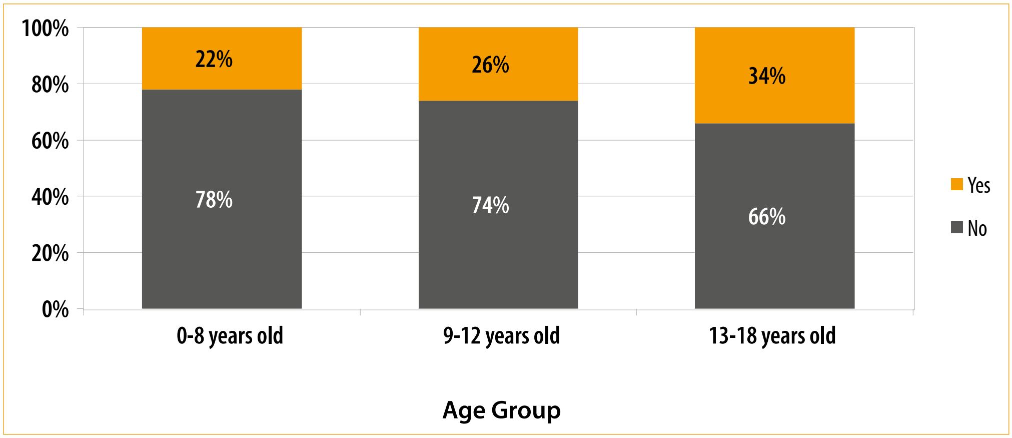
Policy: Schools use…	Member States that have implemented a policy (%)	Member States with no policy or policy not implemented (%)
cloud services.	32	68
secure wifi.	38	62
secure networks.	40	60
secure encryption.	38	62

4.3.3. Do schools monitor their ICT systems: Are students' data safe?

Responses to the survey indicate that in over 60 per cent of the surveyed Member States' schools do not conduct internal or external audits on their ICT systems. This raises the concern that schools' ICT security systems are vulnerable to cyber-attacks, particularly personal data and children's information residing in school-based databases.

Figure 21 shows the findings by age group. On average, only 22 per cent of the surveyed Member States implement a policy to review and audit school ICT systems internally and externally at the early childhood to early primary level (children aged 0-8), 26 per cent have such a policy for the primary school level age group (children aged 9-12) and 34 per cent have such a policy for the secondary school level age group (children aged 13-18).

Figure 21: Percentage of Member States that implement policies to ensure that schools regularly audit the security of school ICT systems



Notably, some of the participating Member States, including Australia, Bhutan, the Cook Islands, Kazakhstan, Nepal, Palau and Samoa do not have policies for the review and audit of the safety and security of their school ICT systems for even one of the three age groups.

These findings suggest that the Member States are not currently making adequate provisions in terms of budget, personnel and training to ensure that the security of school-based ICT systems is not neglected in the implementation of ICT in Education initiatives. This policy gap should be addressed to ensure the security of the data contained in school ICT systems.

4.3.4. Do governments regulate children's ICT use by technical means?

One of the primary means employed by governments to mediate children's use of ICT is the use of technical means such as using filtering software and regulating domestic Internet Service Providers to block, filter and restrict specific types of online content. Taking the sum of all affirmative responses to the question, the responses indicate that 85 per cent of the surveyed Member States use technical means to regulate or filter inappropriate content and/or have monitoring systems in the Member State. Given the prevalence of restrictive and blocking mechanisms, it appears that the Member States view such means as necessary to manage the perceived risks of ICT use among children.

Member States such as Malaysia, Bhutan, Cook Islands and Brunei indicate they have filtering and/or monitoring systems at all levels (local, provincial and national), while Nepal, Lao PDR and Palau do not have any filtering and/or monitoring systems in place.

Kazakhstan has established a variant of the typical content filtering and monitoring mechanism by seeking the collaboration of citizens in building a safer online space for Kazakh-speaking internet users (Box 8).

Box 8: Kazakhstan's Safe Kaznet scheme

The Safe Kaznet scheme was founded by a public organization, the Internet Association of Kazakhstan, and is being implemented in close collaboration with relevant government ministries and representatives of the Kazakhstani internet industry.

The scheme aims to prevent the intrusion of illegal content, including extremist propaganda, terrorist propaganda, and propaganda relating to drugs, pornography and cruel and violent content. The public is encouraged to report applicable locally-hosted content via an online webpage, and the complainants have access to a telephone hotline to allow them to provide feedback and check on the status of their complaints. The stated goal of Safe Kaznet is to popularize the national segment of the internet and promote the development of a harmonious environment that takes into account the interests of all of its users.

The scheme deals with illegal content when it is reported to them by users. After investigating the reported sites, the content may then be taken down by an internet service provider. The reported sites are also forwarded to law enforcement agencies if there are indications that the sites have broken a law.

While this scheme might not be applicable for non-Kazakh websites, it may be a unique approach in tackling the issue of inappropriate content in a particular segment of the internet by attempting to restrict or block access to illegal content that exists in the country's national language. The scheme represents a special approach in that it is founded by a public organization that has close links with the Kazakhstani internet industry, and it facilitates the removal or blocking of inappropriate content even though it does not appear to have explicit powers to do so.

4.3.5. How do governments know that their ICT policies work?

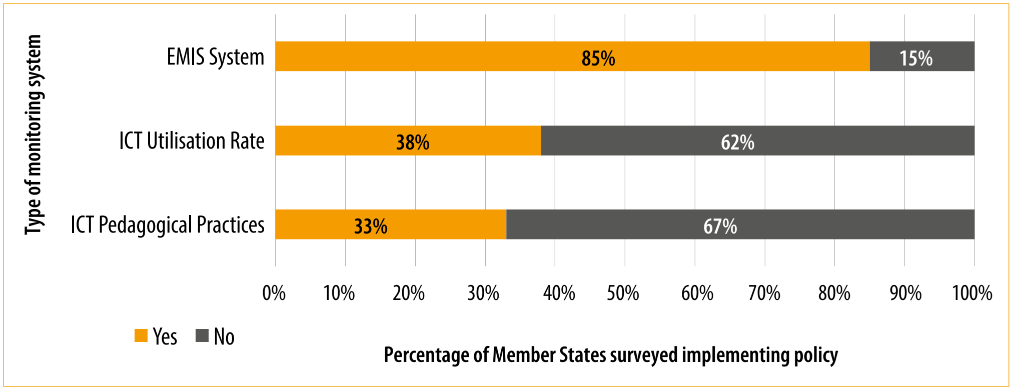
Education Management Information Systems (EMIS) compile and report relevant and timely information that is required for policy planning and analysis, and for systems monitoring and evaluation (Hua and Herstein, 2003). They are useful as they enable information-based decision-making by education policy-makers.

The responses to the survey indicate that 85 per cent of the surveyed Member States have established an EMIS (Figure 22). In more than two-thirds of these Member States, the EMIS has existed for at least five years.

The survey responses indicate that only 38 per cent of the participating Member States have a national mechanism to monitor ICT utilization rates in schools (Figure 22). Most of the Member States with such a mechanism in place share the information with local school leaders or provincial leaders.

Similarly, only 33 per cent of the surveyed Member States have a national system to assess the effectiveness of pedagogical practices in the use of ICT in schools (Figure 22). Most of these Member States share the information with local school leaders.

Figure 22: Percentage of Member States implementing/not implementing systems for assessment, monitoring and evaluation, by type of system



While recognizing that the survey questions do not assess the quality of the EMIS established by the Member States, the responses suggest that most of the surveyed Member States have at least put in place a basic system for data collection that can guide evidence-based policy-making.

Of the Member States that have an EMIS, only 40 per cent use it to obtain information relating to cyber safety policies and practices in schools. Thus, most of these Member States have not expanded the scope of the EMIS to include specific indicators on cyber safety. Including such indicators in the EMIS would assist Member States in monitoring and evaluating the efficacy and impact of national, state, provincial and local level implementation of cyber wellness policies and digital citizenship education.

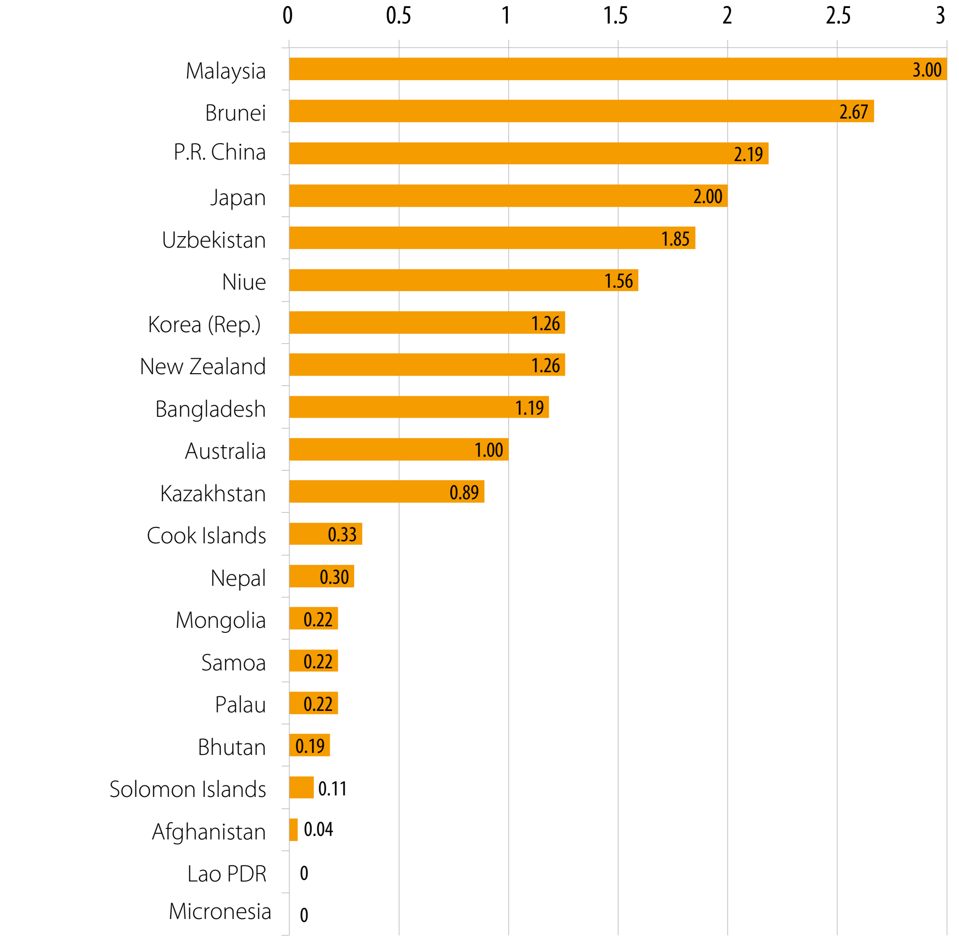
Exceptional Member States that have all three national systems (EMIS, mechanism for monitoring ICT utilization and mechanism for measuring the effectiveness of pedagogical practices) in place in the formal education system include Bangladesh, the Cook Islands, Malaysia, Korea (Rep.) and Uzbekistan.

The Member States that currently lack policies related to monitoring and evaluation mechanisms/programmes and the provision of corresponding resources for implementation should consider developing such policies as they would provide evidence required for effective national policies.

Summary

Figure 23 shows the overall readiness of each Member State regarding technical infrastructure (i.e. the mean scores to questions in Infrastructure category). Half of the participating Member States score an average of less than 1 (Figure 23). This indicates that those Member States either do not have technical infrastructure policies or they do have such policies but they are not implemented. The Member States with the highest scores, indicating that they have comprehensive policies that have also been implemented, are Brunei (2.67) and Malaysia (3). One Member State that stands out is Uzbekistan (1.85), which demonstrates a relatively high level of policy readiness despite being among the region's lower income countries and having a lower level of ICT development compared with many other Member States in the region.

Figure 23: Overall technical infrastructure policy readiness of participating Member States

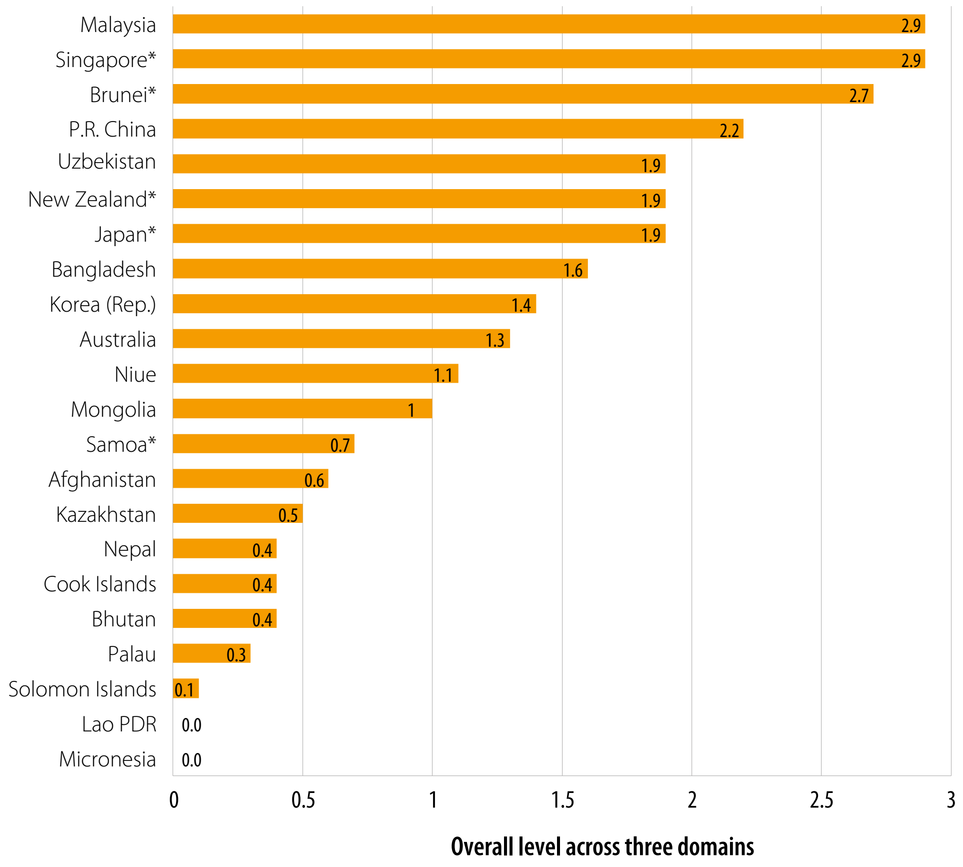


Note: Singapore was unable to submit responses in this category.

4.4. Summary of findings

Figure 24 illustrates the participating Member States' respective levels of overall "policy readiness" based on each Member State's mean score across all the survey questions in the three categories.

Figure 24: Overall policy readiness of participating Member States



Note: As specified above, Japan, Singapore, New Zealand, Samoa and Brunei were unable to provide responses to various questions in the survey.

The data suggest a strong connection between participating Member States' income levels and their level of policy "readiness", such that the high income and upper-middle income Member States tend to have higher overall policy readiness in all three research categories, compared to their lower income counterparts. However, it must be noted that Bangladesh and Uzbekistan exhibit strong policy readiness despite being lower-middle-income countries and being ranked at 115th and 144th in the IDI 2015. In the same manner, while some of the surveyed Member States have developed relevant national policies, these have not necessarily translated to actual nationwide implementation. This is possibly due to local political and implementation structures, commitment priorities and/or a lack of resources and internal expertise.

The key findings of the policy review were as follows:

- **Member States recognize the importance of equipping children with ICT skills and providing basic infrastructure.**

  The ministries of education in about 75 per cent of the participating Member States have policies promoting basic ICT literacy skills among children and also have policies promoting at least one computer lab per school at the secondary school level. However, the Member States give less attention to training beyond basic ICT literacy. More advanced ICT skills would promote more sophisticated media and information literacy, such as interactive and critical use of media as well as constructive online participation and content creation.

- **A multi-sector approach is taken by many Member States in the development of cyber safety or privacy policies, but it could be further improved.**

  Two-thirds of the participating Member States have involved experts from one or more of four key sectors (law enforcement, health, education and cyber security) in the development of cyber safety and privacy policies. But recent research indicates that Member States should create a dialogue that also includes children's perspectives on the opportunities and risks of ICT use and increasing digital literacy skills, while developing digital citizenship values.

- **Policies need to be improved in supporting teachers to be adequately equipped to teach with ICT.**

  Overall, the policies that most of the surveyed Member States have implemented to support the development of teachers' basic ICT skills, alongside cyber wellness and cyber security competencies, can be improved. Furthermore, most teacher development policies relating to ICT use are not fully implemented. Without the basic knowledge and skills to use ICT and to utilize ICT in teaching, teachers cannot be effective in nurturing students to be active digital citizens who use ICT safely, effectively and responsibly.

- **Member States' policies to promote ICT opportunities mature alongside policies that address potential risks.**

  Survey responses show that a Member State's policy readiness to empower children to embrace ICT opportunities is strongly and positively correlated with its policy readiness to address potential risks ($r > 0.9$). It is evident among surveyed Member States that opportunity-oriented policies and safety-oriented policies go hand in hand.

- **Member States focus on children in secondary school, much less on younger children.**

  Only around half of the participating Member States have policies to promote basic ICT skills and digital citizenship among children aged 0-8 years old. Furthermore, many countries have not established the technical infrastructure required to facilitate access and use of ICT among younger children.

- **Half of the Member States lack security measures and therefore have vulnerable school ICT systems.**

  Only 55 per cent of the participating Member States have policies in place for secure WiFi, networks and encryption at the secondary school level, while only 48 per cent have such policies at the early childhood to early primary school age group level and only 51 per cent have them at the primary school age group level. These findings suggest that a significant number of school ICT systems in the Asia-Pacific region are vulnerable to malicious attacks or unauthorized intrusions; thus the storage and transmission of private information is at risk. School-based ICT systems are potentially vulnerable to malicious attacks targeting students' personal information and data.

- **Audits and reviews of school ICT security systems are lacking.**

  Over 60 per cent of the participating Member States lack policies to enable schools to regularly review and audit the safety and security of their ICT systems. This could potentially lead to unauthorized intrusions or malicious attacks.

- **Most Member States in the Asia-Pacific region block content and place restrictions on access to content.**

  More than 80 per cent of the participating Member States employ content filtering systems and/or monitoring systems at the local, provincial and/or national levels. These Member States view these systems as being necessary for reducing the risks of ICT use among children.

- **Most Member States lack systems for monitoring and evaluating digital citizenship policies and procedures.**

  Monitoring and evaluation of programmes is an important aspect of evidence-based policy creation and implementation. However, 73 per cent of the Member States that participated in the survey do not have assessment systems in place to measure the efficacy of their digital citizenship policies and procedures. Furthermore, while 85 per cent of the Member States have an education management information system (EMIS) in place, only 40 per cent of those Member States use the EMIS to manage information relating to students' cyber safety.

- **The needs of the Member States in the Asia-Pacific region are diverse.**

  The findings reinforce the results of other research regarding the vast disparity and variation seen in Asia-Pacific with regard to ICT technical resources, infrastructure capabilities and integration of ICT into education. The findings of the survey also demonstrate that Member States in the Asia-Pacific region occupy the entire spectrum of national ICT policies in terms of "leadership and accountability", "education" and "technical infrastructure" – ranging from Member States that have no policies (i.e. Level 0) relating to the survey's three research categories to Member States that have policies that are not only implemented but are also monitored and evaluated (i.e. Level 3).

- **Member States lack adequate data on children's behaviour, perceptions and usage of ICT both nationally and regionally.**

  There is limited research establishing the baseline ICT usage among children or about their online behaviour, the quality and nature of children's ICT use when in school, or ICT use among family members and in the wider community. Almost half (47 per cent) of the participating Member States do not have a national programme to promote the use of research to inform and support policy, and if one is in place, it is not used consistently. The lack of research and locally-relevant data indicates that policies are developed based on assumptions or on research that may not be locally applicable.

5. Conclusions

This policy review has revealed key aspects of policy-making in the region with regard to children's safe, effective and responsible use of ICT and with regard to fostering children's digital citizenship.

The surveyed Asia-Pacific Member States have acknowledged the importance of ICT in Education, and already promote and implement policies to impart basic ICT literacy skills to children. They also largely provide the basic technical infrastructure to foster the use of ICT in schools. The review also found that while they often rely on technical means to block content and restrict access to content online, many of the participating Member States have a balanced set of educational policies that encourage ICT opportunities alongside emphasizing safety and minimizing risk. This balanced treatment ensures that opportunities offered by ICT and the internet are not diminished by efforts to improve safety and mitigate the risks that children face.

A number of observations need to be further examined, such as Bangladesh's and Uzbekistan's policies that are significantly more developed than many other participating Member States with similar income and ICT development levels. Bangladesh and Uzbekistan have shown that a comprehensive policy base for fostering children's safe, effective and responsible use of ICT and digital citizenship policies can be built in parallel with economic and ICT development.

There is room for research into the particular reasons for the lack of policies relating to the safe, effective and responsible use of ICT by children in some Member States. It is also worth investigating the reasons and conditions why some Member States have developed policies in all three categories while others have not.

The findings of this policy review leave no doubt that there remains much to be done in terms of developing and implementing policies and practices to foster digital citizenship among children in the Asia-Pacific region. However, the various ongoing actions and initiatives in the region provide inspiration and models. Member States can – through sharing knowledge and through communication and collaboration – adopt best practices, model initiatives and lessons learned to develop policies that will ensure their children are better equipped to benefit from the digital world.

6. Policy recommendations

The findings of this policy review show that there is great diversity in the extent of policy readiness among the surveyed Member States. The findings also highlight the areas in which Member States are progressing well as well as the areas in which the development and implementation of policies can be improved. To this end, the following policy recommendations are proposed:

➲ **Take a balanced approach to ICT.**

Member States should develop national policies for ICT in education that foster digital citizenship in schools, maximize the opportunities afforded by ICT and facilitate the development of ICT infrastructure. At the same time, Member States should employ ICT-related policies that mitigate risks and enhance safety for children.

➲ **Develop basic ICT skills in all children.**

Member States should institute and implement policies that increase ICT literacy skills among children of all age groups (from pre-primary to 18 years old), and provide the adequate technical infrastructure to facilitate such learning.

➲ **Go beyond basic ICT skills.**

Member States should develop and implement education policies that increase provisions for gaining more advanced, higher-order ICT skills, through curricular and extra-curricular activities, so as to enable learners to cope with the changing digital environment. UNESCO's extensive resources on Media and Information Literacy[2] may serve as useful references on this.

➲ **Develop appropriate technical infrastructure for early childhood education.**

Member States should develop and implement education policies and age-appropriate technical infrastructure to increase opportunities for young children (0-8 years old) to access and use ICT.

[2] UNESCO Media and Information Literacy. http://www.unesco.org/new/en/communication-and-information/media-development/media-literacy/mil-as-composite-concept/

- **Incorporate digital citizenship as part of teacher competency standards.**

  Member States can complement their student-focused policies by developing and implementing competency standards that ensure teachers are equipped with basic ICT skills as well as the capacity to teach children about safe, effective and responsible ICT use and digital citizenship. In addition, Member States should support policies that build teachers' capacity to utilize ICT in teaching, so as to increase the opportunities afforded by ICT in schools.

- **Improve the allocation of resources to the security of ICT systems.**

  Member States should ensure that sufficient resources, in terms of budget, personnel and training, are allocated to providing adequate security measures for school-based ICT systems.

- **Establish a nationwide EMIS to improve monitoring and evaluation of digital citizenship policies.**

  One of the advantages of using ICT in teaching and learning is that teachers' and students' use of ICT can be automatically logged, collected and stored, which in turn can be invaluable data sources for evidence-based policy development. A nationwide EMIS with a built-in learning log analytics will serve as an essential element in understanding and monitoring students' digital behaviour and thus support the development of an effective and data-driven digital citizenship programme for children.

- **Adapt programmes and initiatives to local contexts.**

  Every country is different and so are their needs. Member States should develop policies that are adapted to national and local contexts and tailored to the needs of local children.

- **Pursue a multi-stakeholder, multi-sector approach.**

  Member States should consider pursuing public-private partnerships as part of a multi-stakeholder, multi-sector approach that incorporate various perspectives to developing and implementing policies and initiatives relating to children's safe, effective and responsible use of ICT.

7. Way forward

Having examined the state of policy readiness in the Asia-Pacific region, the groundwork has been laid for research on the details of implementing such policies and on how such policies actually affect the target audience, i.e. children, from the ground up, while considering each country's unique context.

The next step in building the evidence base for the Asia-Pacific region would be to obtain and analyse both quantitative and qualitative data on a comparative region-wide basis to establish what and how children are actually doing in their interactions with ICT, namely, their perceptions, actions and reactions towards the opportunities and risks posed by ICT, the factors that drive the choices of children in the Asia-Pacific region and how children's interactions with the wider community of family, caregivers and peers have an effect on or are affected by ICT.

This vital yet massive work requires regional and international cooperation between academics, international organizations, national education authorities, schools and parents, as well as like-minded financial supporters. The Global Kids Online, which is a collaboration between the London School of Economics, UNICEF Office of Research and EU Kids Online, is a great example of such partnership (London School of Economics, 2016).

Given that Member States of the region are at different levels of policy readiness across the three categories of policies, there is potential for the development of a platform on which Member States could share their best practices regionally or sub-regionally. An online resource database and forum could be created through which ministry personnel, policy-makers, NGOs and development partners can consult and share information. Another possibility is the establishment of a region-wide mechanism to allow collaboration through a multi-sector and multi-stakeholder approach to permit a broader and more inclusive process in sharing policy development expertise with counterparts in other Member States.

References

Afshari, M., Bakar, K. A., Su Luan, W., Samah, B. A. and Fooi, F. S. 2009. Factors affecting teachers' use of information and communication technology. *International Journal of Instruction*, Vol. 2. No. 1. pp. 77-104.

Baudouin, P., Nakajima, S., Mahieu, B., Good, B, Milayi, J. and Dor, T. 2014. *Benchmarking of Safer Internet policies in EU Member States and policy indicators: Final Report*. Clapiers, IDATE.

Chaudron, S. 2015. *Young Children (0-8) and Digital Technology: A qualitative exploratory study across seven countries*. Luxembourg, Publications Office of the European Union.

Council of Europe. 2012. *Recommendation CM/Rec (2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services*. Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies.

CyberSecurity Malaysia. 2016. CyberSAFE Malaysia. http://www.cybersafe.my/about.html (Accessed 10 June 2016.)

Department for Children, Schools and Families. 2008. Safer Children in a Digital World: The Report of the Byron Review. Nottingham, Department for Children, Schools and Families, and the Department for Culture, Media and Sport.

Department of Communications and the Arts, Australia. 2015. Leading online safety expert Alastair MacGibbon appointed Children's e-Safety Commissioner. 19 March. http://www.minister.communications.gov.au/paul_fletcher/news/leading_online_safety_expert_alastair_macgibbon_appointed_childrens_e-safety_commissioner#.VrNeq9J96ik (Accessed 10 June 2016.)

Digi CyberSafe Programme. 2015. Empowerment through connectivity: Sustainability report. http://www.digi.com.my/sustainability/pdf/page-focus-etc.pdf (Accessed 10 June 2016.)

European Commission. 2012. *European Strategy for a Better Internet for Children*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, European Commission. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDF (Accessed 10 June 2016.)

_____. 2013. Survey of Schools: ICT in Education. Benchmarking Access, Use and Attitudes to Technology in Europe's Schools. Brussels, European Commission Directorate-General for Communications Networks, Content and Technology.

_____. 2014. *Mapping Safer Internet Policies in the Member States: The Better Internet for Kids (BIK) Map*. Brussels, European Commission Directorate-General for Communications Networks, Content and Technology, European Union.

Gasser, U., Maclay, C. and Palfrey, J. 2010. Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations. Berkman Center Research Publication No. 2010-7; Harvard Public Law Working Paper No. 10-36.

Green, L., Brady, D., Olafsson, K., Hartley, J. and Lumby, C. 2011. Risks and safety for Australian children on the internet: Full findings from the AU Kids Online survey of 9-16 year olds and their parents. Cultural Science, Vol. 4, No. 1, pp. 1-73.

Groupe Spéciale Mobile Association. (2013). *Children's use of mobile phones: An international comparison 2012*. London, Groupe Spéciale Mobile Association (GSMA).

Hua, H. and Herstein, J. 2003. Education Management Information System (EMIS): Integrated Data and Information Systems and Their Implications in Educational Management. Paper presented at the Annual Conference of Comparative and International Education Society. New Orleans, March 2003.

International Centre for the Study of Radicalisation and Political Violence (ICSR). 2009. *Countering Online Radicalisation: A Strategy for Action*. London, ICSR.

International Society for Technology in Education. ISTE Standards. http://www.iste.org/standards/iste-standards (Accessed 10 June 2016.)

International Telecommunications Union. 2015a. *ICT Facts and Figures: The World in 2015*. Geneva, ICT Data and Statistics Division, ITU.

_____. 2015b. *Measuring the Information Society Report 2015*. Geneva, ITU.

Kozma, R. B. 2008. Comparative Analysis of Policies for ICT in Education. J. Voogt and G. Knezek (eds.), *International Handbook of Information Technology in Primary and Secondary Education*. New York, Springer, pp. 1083-96.

Livingstone, S., Haddon, L., Görzig. A. and Ólafsson, K. 2011. *Risks and safety on the internet: The perspective of European children. Full findings*. London, EU Kids Online.

Livingstone, S. and Bulger, M. E. 2013. *A Global Agenda for Children's Rights in the Digital Age*. Florence, UNICEF Office of Research.

Livingstone, S. and Helsper, E. 2007. Gradations in digital inclusion: children, young people and the digital divide. *New Media & Society,* Vol. 9, No. 4, pp. 671-96.

_____. 2010. Balancing opportunities and risks in teenagers' use of the internet: The role of online skills and internet self-efficacy. *New Media & Society,* Vol. 12, No. 2, pp. 309-29.

Livingstone, S., Carr, J. and Byrne, J. 2016. One in Three: Internet Governance and Children's Rights. *Innocenti Discussion Paper*, No. 2016-01, UNICEF Office of Research.

London School of Economics. 2016. Global Kids Online: Children's rights in the digital age. http://www.lse.ac.uk/media@lse/research/Global-Kids-Online.aspx (Accessed 22 April 2016.)

Malaysian Communications and Multimedia Commission. 2015. http://www.klikdenganbijak.my/?lang=en-GB (Accessed 10 June 2016.)

Media Development Authority, Singapore. 2016. What is Media Literacy? http://www.mda.gov.sg/PublicEducation/MediaLiteracy/Pages/MediaLiteracy.aspx (Accessed 10 June 2016.)

Ministry of Education of Singapore. 2014. *2014 Syllabus Cyber Wellness Secondary*. Student Development Curriculum Division. https://www.moe.gov.sg/docs/default-source/document/education/syllabuses/character-citizenship-education/files/2014-cyber-wellness.pdf (Accessed 10 June 2016.)

_____. 2015. 7th Call for Proposals on Cyber Wellness Projects. 10 December. https://www.moe.gov.sg/news/press-releases/7th-call-for-proposals-on-cyber-wellness-projects (Accessed 10 June 2016.)

_____. 2016. Cyber wellness 101. http://ictconnection.moe.edu.sg/cyber-wellness/cyber-wellness-101 (Accessed 10 June 2016.)

NZ On Air. 2015. Children's Media Use Study: How our children engage with media today. http://www.nzonair.govt.nz/document-library/childrens-media-use-study-2015 (Accessed 10 June 2016.)

O'Neill, B. 2014. *Policy Influences and Country Clusters: A Comparative Analysis of Internet Safety Policy Implementation*. London, London School of Economics and EU Kids Online.

OECD. 2012a. *The Protection of Children Online*. Paris, OECD Publishing.

_____. 2012b. *Connected Minds: Technology and Today's Learners*. Paris, Educational Research and Innovation, OECD Publishing.

Ribble, M. 2016. Digital Citizenship - Using Technology Appropriately: Nine Elements. http://www.digitalcitizenship.net/Nine_Elements.html (Accessed 10 June 2016.)

Sefton-Green, J., Marsh, J., Erstad, O. and Flewitt, R. 2016. *Establishing a Research Agenda for the Digital Literacy Practices of Young Children: A White Paper for COST Action IS1410*. http://

digilitey.eu/wp-content/uploads/2015/09/DigiLitEYWP.pdf (Accessed 22 April 2016.)

TheAsianparent Insights. 2014. *Mobile device usage among young kids: A Southeast Asia Study.* Singapore, TheAsianparent and Tickled Media.

ThinkUKnow Australia. Welcome to the ThinkUKnow website. http://www.thinkuknow.org.au/site (Accessed 10 June 2016.)

The Open University. 2012 Digital and Information Literacy Framework. http://www.open.ac.uk/libraryservices/subsites/dilframework (Accessed 10 June 2016.)

Third, A., Bellerose, D., Dawkins, U., Keltie, E., and Pihl, K. 2014. Children's Rights in the Digital Age: A Download from children around the world. 2nd edition. Melbourne, Young and Well Cooperative Research Centre.

Third, A., Forres-Lawrence, P. and Collier, A. 2014. *Addressing the Cyber Safety Challenge: From Risk to Resilience*. Melbourne, Telstra.

UNESCO Institute for Statistics. 2014. *Information and Communication Technology (ICT) in Education in Asia: A comparative analysis of ICT integration and e-readiness in schools across Asia*. Montreal, UIS.

United Nations Economic and Social Council. 2015. *Digital Development: Report of the Secretary-General.* 23 February. E/CN.16/2015/2

Office of the United Nations High Commissioner for Human Rights. 2014. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.*

UNESCO. 2015a. *Education 2030: Incheon Declaration and Framework for Action – Towards inclusive and equitable education and lifelong learning for all.* World Education Forum, Incheon, Korea, 19-22 May 2015. http://unesdoc.unesco.org/images/0024/002432/243278e.pdf (Accessed 4 June 2016.)

_____. 2015b. *Fostering Digital Citizenship through Safe and Responsible Use of ICT: A review of current status in Asia and the Pacific as of December 2014.* Bangkok, UNESCO.

UNICEF. 2013. *Child well-being in rich countries: A comparative overview.* Florence, UNICEF Office of Research.

Wilson, C., Grizzle, A., Tuazon, R., Akyempong, K. and Cheung, C.-K. 2011. *Media and Information Literacy Curriculum for Teachers*. Paris, UNESCO.

Appendix 1. Participating Member States

Member State	Organization
Afghanistan	Ministry of Education
Australia	Office of the Children's eSafety Commissioner
Bangladesh	Bangladesh Bureau of Educational Information and Statistics
Bhutan	Ministry of Education
Brunei	Ministry of Education
P.R. China	Beijing Normal University
Cook Islands	Ministry of Education
Japan	National Commission for UNESCO
Kazakhstan	Internet Association of Kazakhstan
Lao PDR	Ministry of Education and Sports
Malaysia	Ministry of Education
Micronesia	National Department of Education
Mongolia	Institute of Teacher's Professional Development
Nepal	Department of Education (Bhaktapur)
New Zealand	Netsafe
Niue	National Commission for UNESCO
Palau	Ministry of Education
Korea (Rep.)	Korea Educational and Research Information Service
Samoa	Samoa National Commission for UNESCO
Singapore	Nanyang Technological University Ministry of Education
Solomon Islands	Ministry of Education and Human Resource Development
Uzbekistan	Ministry of Public Education

Appendix 2. Survey instrument

Introduction

Thank you for participating in this survey. Your responses will provide a valuable snapshot of how digital citizenship is being considered in the Asia-Pacific region at the national level. The data gathered will inform policy recommendations on the issues of the ethical, safe, and responsible use of ICT and in building the education sector's capacity in fostering digital citizenship among children.

The survey should take less than 30 minutes to complete and includes four sections: 1) Leadership and Accountability, 2) Education, 3) Technical Infrastructure, and 4) Other Information. There are three sub-sections under "Education" and "Technical Infrastructure" – (a) early childhood to early primary (0-8 years old); (b) primary (9-12 years old); and (c) secondary (13-18 years old). The nominated respondent is encouraged to forward the survey to relevant departments/personnel in order to gather well-informed responses (e.g. the sub-section on early childhood to early primary should be responded by the early childhood care and education department).

Through this survey and other data-gathering methods (i.e. document analysis, interviews, desk review) our goal is to (a) collate, synthesize, and transmit the experiences and resources of existing key players in this area, and (b) provide educational policy review and recommendations for the member states across the Asia-Pacific region to guide country-specific roll-out of the customized initiatives in their respective countries.

Based on the findings, UNESCO aims to develop a regional guide for educators to build their capability in fostering digital citizenship among children. It is hoped that this project will contribute to UNESCO's current efforts of equipping citizens with competencies to engage confidently and productively in global discourse and development.

Cloud services — a centralized storage system, usually through a server or multiple servers, that can be accessed publicly, privately, or a combination thereof. Clouds in educational settings should be password protected with robust security measures.

Cyber wellness — refers to positive well-being and productive engagement with the Internet and related tools, especially social media oriented interactions. Often used interchangeably with "cybersafety."

Education Management Information System (EMIS) — type of system that is designed to manage digital information about an education system. An EMIS is a repository for data collection, processing, analyzing and reporting of educational information including schools, students, teachers and staff.

Encryption — encoding of messages and/or software to prevent unintended individuals to intercept or read protected messages or software.

Lifelong learning — refers to learning activities that occur both inside and outside of the classroom, and through formal and/or informal modalities of learning.

Assessment of Digital Citizenship and Cyber Wellness in Asia-Pacific Schools

1. Leadership and Accountability

This section aims to assess what is being done on a national level to promote ethical, safe, and responsible use of ICT and in building the education sector's capacity in fostering digital citizenship among children. Specifically, how have national leaders articulated a commitment to digital citizenship and cyber wellness such that school systems recognize and implement these elements as components in their curriculum and school culture?

What country do you represent?

1.1 Please answer accordingly.

	Level 0: No campaigns	Level 1: Campaigns are developed with multiple stakeholders	Level 2: Campaigns are developed and distributed through multiple stakeholder groups	Level 3: Campaigns are distributed through multiple stakeholder groups & evaluated for effectiveness
National campaigns are conducted to promote safe and responsible ICT use.	○	○	○	○
National campaigns are conducted to inform communities and stakeholders about the process of reporting cases of ICT abuse and misuse.	○	○	○	○

1.2 Please answer accordingly.

	Level 0: No involvement	Level 1: Little/ inconsistent involvement	Level 2: Consistent involvement	Level 3: Consistent involvement that is tracked for effectiveness
Law enforcement personnel are involved in the development of cyber safety or privacy policies.	○	○	○	○
Health professionals are involved in the development of cyber safety or privacy policies.	○	○	○	○
Education experts are involved in the development of cyber safety or privacy policies.	○	○	○	○
Cyber security experts are involved in the development of cyber safety or privacy policies.	○	○	○	○

1.3 Please answer accordingly.

	Level 0: No agency/provision/ program is in place	Level 1: An agency/provision/ programis in place, but it is not consistently utilized	Level 2: An agency/provision/ program is in place, but it is not tracked for effectiveness	Level 3: An agency/provision/ program is in place, and it is tracked for effectiveness
There is a national agency in place to coordinate campaigns and efforts among various departments.	○	○	○	○
There is a provision of national budget to support digital citizenship policies and procedures.	○	○	○	○
There is a national program in place to promote the use of research to inform/ support policy.	○	○	○	○
There is an assessment program in place to measure the efficacy of digital citizenship policies and procedures.	○	○	○	○

Assessment of Digital Citizenship and Cyber Wellness in Asia-Pacific Schools

2.1 Education - early childhood to early primary (0-8 years old)

This section aims to assess what is being done on a national level to promote ethical, safe, and responsible use of ICT and in building the education sector's capacity in fostering digital citizenship among **children aged 0-8 years old (early childhood to early primary school level)**. Specifically, what educational activities, e.g., curriculum, have formally integrated digital citizenship and cyber wellness into their formal instruction and learning opportunities for learners and teachers?

2.1.1 Ministry of Education has policies/programmes/resources **targeting caregivers (parents, guardians, teachers)** that promote...

	Level 0: No policy is in place	Level 1: There is a policy, but it is not implemented	Level 2: There is a policy that is implemented (budget/ resources are provided)	Level 3: There is a policy that is implemented and monitored/ evaluated
..guidance on posting information (how much, what type) about children.	○	○	○	○
...securing personal, school, and family data.	○	○	○	○
...training for teachers and school ICT staff on use of ICT provisions in school.	○	○	○	○
...appropriate adult mediation on children's ICT use through the use of content filtering services.	○	○	○	○
...appropriate adult mediation on children's ICT use through guidance on healthy limits of screen time	○	○	○	○

	Level 0: No policy is in place	Level 1: There is a policy, but it is not implemented	Level 2: There is a policy that is implemented (budget/ resources are provided)	Level 3: There is a policy that is implemented and monitored/ evaluated
....appropriate adult mediation on children's ICT use in preventionand intervention for pornography, gaming, and other addictive behaviour.	○	○	○	○
...national standards for teacher preparation that include ICT literacy skills, cyber wellness and cyber security skills and competencies.	○	○	○	○
...faculty development programmes on ICT use for learning that include cyber wellness and cyber security components.	○	○	○	○

2.1.2. Ministry of Education has policies/programmes/resources **targeting students** that promote...

	Level 0: no policy is in place	Level 1: there is a policy but is not implemented	Level 2: there is a policy that is implemented (budget/ resources are provided)	Level 3: there is a policy that is implemented and monitored/ evaluated
...basic ICT literacy skills.	○	○	○	○
...digital storytelling, computer coding, and production of other ICT outputs.	○	○	○	○
...healthy limits of screen time / healthy balance between online and offline activities.	○	○	○	○
...building and maintaining a positive digital reputation.	○	○	○	○
...privacy skills and competencies.	○	○	○	○
...cyber security skills and competencies.	○	○	○	○
...creating, communicating and collaborating online / safe and responsible social networking, including content viewing and sharing.	○	○	○	○
...ethical use of creative content (content owned by others).	○	○	○	○
...appropriate response to cyber-bullying.	○	○	○	○

2.1.3 Ministry of Education has policies/programmes/resources **targeting individual schools** that promote...

	Level 0: no policy is in place	Level 1: there is a policy but is not implemented	Level 2: there is a policy that is implemented (budget/ resources are provided)	Level 3: there is a policy that is implemented and monitored/ evaluated
..."lifelong learning" activities with digital-age learning tools and content.	○	○	○	○
...use of student-owned devices.	○	○	○	○
...integrating innovative ICT-supported learning initiatives into curricula activities.	○	○	○	○
...incorporating safe and responsible use of ICT/cyber wellness in the curriculum.	○	○	○	○
...incorporating safe and responsible use of ICT/cyber wellness in co- curricular or extracurricular activities.	○	○	○	○
...use and publication of digital and video images.	○	○	○	○
...use of Acceptable Use Policies (AUP) by school stakeholders.	○	○	○	○
...Acceptable Use Policies (AUP) that include sanctions for ICT abuse and misuse.	○	○	○	○

	Level 0: no policy is in place	Level 1: there is a policy but is not implemented	Level 2: there is a policy that is implemented (budget/ resources are provided)	Level 3: there is a policy that is implemented and monitored/ evaluated
...formation of multi-stakeholder cyber wellness committees.	○	○	○	○
...conduct of safe and responsible use of ICT/cyber wellness sessions with caregivers.	○	○	○	○
...prevention and intervention for pornography, gaming, and other addictive behaviour.	○	○	○	○

2.2 Education - primary (9-12 years old)

This section aims to assess what is being done on a national level to promote ethical, safe, and responsible use of ICT and in building the education sector's capacity in fostering digital citizenship among **children aged 9-12 years old (primary school level)**. What educational activities, e.g., curriculum, have formally integrated digital citizenship and cyber wellness into their formal instruction and learning opportunities for learners and teachers?

2.2.1 Ministry of Education has policies/programmes/resources **targeting caregivers (parents, guardians, teachers)** that promote...

	Level 0: No policy is in place	Level 1: There is a policy, but it is not implemented	Level 2: There is a policy that is implemented (budget/ resources are provided)	Level 3: There is a policy that is implemented and monitored/ evaluated
...guidance on posting information (how much, what type) about children.	○	○	○	○
...securing personal, school, and family data.	○	○	○	○
...training for teachers and school ICT staff on use of ICT provisions in school.	○	○	○	○
...appropriate adult mediation on children's ICT use through the use of content filtering services.	○	○	○	○
...appropriate adult mediation on children's ICT use through guidance on healthy limits of screen time.	○	○	○	○

	Level 0: No policy is in place	Level 1: There is a policy, but it is not implemented	Level 2: There is a policy that is implemented (budget/ resources are provided)	Level 3: There is a policy that is implemented and monitored/ evaluated
...appropriate adult mediation on children's ICT use in prevention and intervention for pornography, gaming, and other addictive behaviour.	○	○	○	○
...national standards for teacher preparation that include ICT literacy skills, cyber wellness and cyber security skills and competencies.	○	○	○	○
...faculty development programmes on ICT use for learning that include cyber wellness and cyber security components.	○	○	○	○

2.2.2 Ministry of Education has policies/programmes/resources **targeting students** that promote...

	Level 0: no policy is in place	Level 1: there is a policy but is not implemented	Level 2: there is a policy that is implemented (budget/ resources are provided)	Level 3: there is a policy that is implemented and monitored/ evaluated
...basic ICT literacy skills.	○	○	○	○
...digital storytelling, computer coding, and production of other ICT outputs.	○	○	○	○
...healthy limits of screen time / healthy balance between online and offline activities.	○	○	○	○
...building and maintaining a positive digital reputation.	○	○	○	○
...privacy skills and competencies.	○	○	○	○
...cyber security skills and competencies.	○	○	○	○
...creating, communicating and collaborating online / safe and responsible social networking, including content viewing and sharing.	○	○	○	○
...ethical use of creative content (content owned by others).	○	○	○	○
...appropriate response to cyber-bullying.	○	○	○	○

2.2.3 Ministry of Education has policies/programmes/resources **targeting individual schools** that promote...

	Level 0: no policy is in place	Level 1: there is a policy but is not implemented	Level 2: there is a policy that is implemented (budget/ resources are provided)	Level 3: there is a policy that is implemented and monitored/ evaluated
..."lifelong learning" activities with digital-age learning tools and content.	○	○	○	○
...integrating innovative ICT-supported learning initiatives into curricula activities.	○	○	○	○
...incorporating safe and responsible use of ICT/cyber wellness in the curriculum.	○	○	○	○
...incorporating safe and responsible use of ICT/cyber wellness in co- curricular or extracurricular	○	○	○	○
...use of student-owned devices.	○	○	○	○
...use and publication of digital and video images.	○	○	○	○
...use of Acceptable Use Policies (AUP) by school stakeholders.	○	○	○	○
...Acceptable Use Policies (AUP) that include sanctions for ICT abuse and misuse.	○	○	○	○
...formation of multi-stakeholder cyber wellness committees.	○	○	○	○

	Level 0: no policy is in place	Level 1: there is a policy but is not implemented	Level 2: there is a policy that is implemented (budget/ resources are provided)	Level 3: there is a policy that is implemented and monitored/ evaluated
...conduct of safe and responsible use of ICT / cyber wellness sessions with caregivers.	○	○	○	○
...prevention and intervention for pornography, gaming, and other addictive behaviour.	○	○	○	○

Assessment of Digital Citizenship and Cyber Wellness in Asia-Pacific Schools

2.3 Education - secondary (13-18 years old)

This section aims to assess what is being done on a national level to promote ethical, safe, and responsible use of ICT and in building the education sector's capacity in fostering digital citizenship among **children aged 13-18 years old (secondary school level)**. What educational activities, e.g., curriculum, have formally integrated digital citizenship and cyber wellness into their formal instruction and learning opportunities for learners and teachers.

2.3.1 Ministry of Education has policies/programmes/resources **targeting caregivers (parents, guardians, teachers)** that promote...

	Level 0: No policy is in place	Level 1: There is a policy, but it is not implemented	Level 2: There is a policy that is implemented (budget/ resources are provided)	Level 3: There is a policy that is implemented and monitored/ evaluated
...guidance on posting information (how much, what type) about children.	○	○	○	○
...securing personal, school, and family data.	○	○	○	○
...training for teachers and school ICT staff on use of ICT provisions in school.	○	○	○	○
...appropriate adult mediation on children's ICT use through the use of content filtering services.	○	○	○	○
...appropriate adult mediation on children's ICT use through guidance on healthy limits of screen time.	○	○	○	○

	Level 0: No policy is in place	Level 1: There is a policy, but it is not implemented	Level 2: There is a policy that is implemented (budget/ resources are provided)	Level 3: There is a policy that is implemented and monitored/ evaluated
...appropriate adult mediation on children's ICT use in prevention and intervention for pornography, gaming, and other addictive behaviour.	○	○	○	○
...national standards for teacher preparation that include ICT literacy skills, cyber wellness and cyber security skills and competencies.	○	○	○	○
...faculty development programmes on ICT use for learning that include cyber wellness and cyber security components.	○	○	○	○

2.3.2 Ministry of Education has policies/programmes/resources **targeting students** that promote...

	Level 0: no policy is in place	Level 1: there is a policy but is not implemented	Level 2: there is a policy that is implemented (budget/ resources are provided)	Level 3: there is a policy that is implemented and monitored/ evaluated
...basic ICT literacy skills.	○	○	○	○
...digital storytelling, computer coding, and production of other ICT outputs.	○	○	○	○
...healthy limits of screen time / healthy balance between online and offline activities.	○	○	○	○
...building and maintaining a positive digital reputation.	○	○	○	○
...privacy skills and competencies.	○	○	○	○
...cyber security skills and competencies.	○	○	○	○
...creating, communicating and collaborating online / safe and responsible social networking, including content viewing and sharing.	○	○	○	○
...ethical use of creative content (content owned by others).	○	○	○	○
...appropriate response to cyber-bullying.	○	○	○	○

2.3.3 Ministry of Education has policies/programmes/resources **targeting individual schools** that promote...

	Level 0: no policy is in place	Level 1: there is a policy but is not implemented	Level 2: there is a policy that is implemented (budget/ resources are provided)	Level 3: there is a policy that is implemented and monitored/ evaluated
..."lifelong learning" activities with digital-age learning tools and content.	○	○	○	○
...integrating innovative ICT-supported learning initiatives into curricula activities.	○	○	○	○
...incorporating safe and responsible use of ICT/cyber wellness in the curriculum.	○	○	○	○
...incorporating safe and responsible use of ICT/cyber wellness in co- curricular or extracurricular activities.	○	○	○	○
...use of student-owned devices.	○	○	○	○
...use and publication of digital and video images.	○	○	○	○
...use of Acceptable Use Policies (AUP) by school stakeholders.	○	○	○	○
...Acceptable Use Policies (AUP) that include sanctions for ICT abuse and misuse.	○	○	○	○

	Level 0: no policy is in place	Level 1: there is a policy but is not implemented	Level 2: there is a policy that is implemented (budget/ resources are provided)	Level 3: there is a policy that is implemented and monitored/ evaluated
...formation of multi-stakeholder cyber wellness committees.	○	○	○	○
...conduct of safe and responsible use of ICT / cyber wellness sessions with caregivers.	○	○	○	○
...prevention and intervention for pornography, gaming, and other addictive behaviour.	○	○	○	○

3. Technical Infrastructure

This section aims to assess what is being done on a national level to build sound technical infrastructure in the education sector to promote the ethical, safe, and responsible use of ICT and foster digital citizenship among children. Beyond the technical support that school infrastructures are expected to provide, they could also serve to provide the architecture to support sound digital citizenship and cyber wellness environments. In what ways do your schools provide broad technical support for digital citizenship and cyber wellness?

3.1 Please answer with respect to **early childhood to early primary school level (i.e. children from 0 to 8 years old).**

	Level 0: There is no policy in place	Level 1: There is a policy, but it is not implemented	Level 2: There is a policy that is implemented (budget/ resources are provided)	Level 3: There is a policy that is implemented and monitored/ evaluated
Schools provide at least the minimum number of computers per school (e.g. computer: student ratio is greater than one computer lab per school).	○	○	○	○
School's minimum bandwidth requirement is set at the national level.	○	○	○	○
Schools use cloud services.	○	○	○	○
Schools use secured wifi.	○	○	○	○
Schools use secured networks.	○	○	○	○
Schools use secured encryption.	○	○	○	○

	Level 0: There is no policy in place	Level 1: There is a policy, but it is not implemented	Level 2: There is a policy that is implemented (budget/ resources are provided)	Level 3: There is a policy that is implemented and monitored/ evaluated
Schools regularly review and audit the safety and security of school ICT systems with oversight from senior leaders.	○	○	○	○
Schools augment internal reviews with rigorous externaleviews of the security of school systems.	○	○	○	○
Budgets support ICT technical personnel for schools to ensure policies are observed.	○	○	○	○

3.2 Please answer with respect to **primary school level (i.e. children from 9 to 12 years old)**.

	Level 0: There is no policy in place	Level 1: There is a policy, but it is not implemented	Level 2: There is a policy that is implemented (budget/ resources are provided)	Level 3: There is a policy that is implemented and monitored/ evaluated
Schools provide at least the minimum number of computers per school (e.g. computer: student ratio is greater than one computer lab per school).	○	○	○	○
School's minimum bandwidth requirement is set at the national level.	○	○	○	○
Schools use cloud services.	○	○	○	○
Schools use secured wifi.	○	○	○	○
Schools use secured networks.	○	○	○	○
Schools use secured encryption.	○	○	○	○
Schools regularly review and audit the safety and security of school ICT systems with oversight from senior leaders.	○	○	○	○

	Level 0: There is no policy in place	Level 1: There is a policy, but it is not implemented	Level 2: There is a policy that is implemented (budget/ resources are provided)	Level 3: There is a policy that is implemented and monitored/ evaluated
Schools augment internal reviews with rigorous external reviews of the security of school systems.	○	○	○	○
Budgets support ICT technical personnel for schools to ensure policies are observed.	○	○	○	○

3.3 Please answer with respect to **secondary school level (i.e. children from 13 to 18 years old)**.

	Level 0: There is no policy in place	Level 1: There is a policy, but it is not implemented	Level 2: There is a policy that is implemented (budget/ resources are provided)	Level 3: There is a policy that is implemented and monitored/ evaluated
Schools provide at least the minimum number of computers per school (e.g. computer: student ratio is greater than one computer lab per school).	○	○	○	○
School's minimum bandwidth requirement is set at the national level.	○	○	○	○
Schools use cloud services.	○	○	○	○
Schools use secured wifi.	○	○	○	○
Schools use secured networks.	○	○	○	○
Schools use secured encryption.	○	○	○	○
Schools regularly review and audit the safety and security of school ICT systems with oversight from senior leaders.	○	○	○	○
Schools augment internal reviews with rigorous external reviews of the security of school systems.	○	○	○	○
Budgets support ICT technical personnel for schools to ensure policies are observed.	○	○	○	○

This sub-section aims to assess the status of national technical infrastructure.

3.4 Has a National Educational Management Information System (EMIS) been established?

○ Yes

○ No

3.5 If so, how long has the EMIS been in place?

○ Five years

○ Ten years

○ Longer than ten years

○ N/A

3.6 Does the EMIS include acquisition of information on cyber safety?

○ Yes

○ No

○ N/A

3.7 Have content filtering and/or monitoring systems been established? (please check ALL that apply)

○ No

○ Yes, at National Levels

○ Yes, at Provincial Levels

○ Yes, at Local Levels

3.8 Are school-based ICT systems audited for safety and security? (please check the ONE that best matches your system)

○ No

○ Yes, daily

○ Yes, weekly

○ Yes, monthly

○ Yes, quarterly

○ Yes, twice a year

○ Yes, annually

3.9 Has an agency been established to review products and services for security and safety before products can be used in schools?

○ Yes

○ No

3.10 If yes, please identify agency:

□

3.11 Is a national-level mechanism in place to monitor ICT utilization rate in schools?

○ Yes

○ No

3.12 If yes, is this information shared with school leaders? (please check ALL that apply)

○ N/A

○ Yes, with provincial leaders

○ Yes, with local school leaders

3.13 Is a national-level system in place to assess effective pedagogical practices in the use of ICT in schools?

○ Yes

○ No

3.14 If yes, is this information shared with school leaders? (please check ALL that apply)

○ N/A

○ Yes, with provincial school leaders

○ Yes, with local school leaders

Assessment of Digital Citizenship and Cyber Wellness in Asia-Pacific Schools

4. Other Information

We hope to conduct case studies of various programmes/ initiatives that are successfully implementing digital citizenship. Below, please identify a program (at the national, community, or school level) that you feel best exemplifies good digital citizenship and cyber wellness initiatives. (We may contact the program office to feature them in our study.)

Programme Name:

Indicate if: National,
Community, or School Level

Lead Organization:

Address:

City/Town

State/Province

ZIP/Postal Code

Country

Email Address

Phone Number

Please provide any links or documents that you believe may be helpful to this project:

Please share any comments that you believe are useful to this project:

Are you available for a video, phone or email interview for follow-up questions and/or clarifications?

○ Yes

○ No thank you

If yes, please provide your contact information below:

Email:	
Phone:	
Skype:	

Thank you again for taking time to complete this survey. If you have any questions or concerns, please contact the UNESCO Bangkok team.

Appendix 3. Responses to survey questions

Category: Leadership and accountability

Legend:

Q1.1: Level 0: No campaigns

Level 1: Campaigns are developed with multiple stakeholders

Level 2: Campaigns are developed and distributed through multiple stakeholder groups

Level 3: Campaigns are distributed through multiple stakeholder groups & evaluated for effectiveness

Q1.2: Level 0: No involvement

Level 1: Little/inconsistent involvement

Level 2: Consistent involvement

Level 3: Consistent involvement that is tracked for effectiveness

Q1.3: Level 0: No agency/provision/programme is in place

Level 1: An agency/provision/programme is in place, but it is not consistently utilized

Level 2: An agency/provision/programme is in place, but it is not tracked for effectiveness

Level 3: An agency/provision/programme is in place, and it is tracked for effectiveness

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	1.1		1.2 Please answer accordingly.				1.3 Please answer accordingly.			
	National campaigns are conducted to promote safe and responsible ICT use	National campaigns are conducted to inform communities and stakeholders about the process of reporting cases of ICT abuse and misuse.	Law enforcement personnel are involved in the development of cyber safety or privacy policies.	Health professionals are involved in the development of cyber safety or privacy policies.	Education experts are involved in the development of cyber safety or privacy policies.	Cyber security experts are involved in the development of cyber safety or privacy policies.	There is a national agency in place to coordinate campaigns and efforts among various departments.	There is a provision of national budget to support digital citizenship policies and procedures.	There is a national programme in place to promote the use of research to inform / support policy.	There is an assessment programme in place to measure the efficacy of digital citizenship policies and procedures.
Korea (Rep.)	2	2	2	2	2	2	3	3	2	0
Japan	2	2	NR	NR	NR	NR	NR	NR	NR	NR
Australia	2	2	2	1	2	2	0	0	1	1
New Zealand	2	3	3	3	3	3	3	2	3	2
Singapore	3	3	3	3	3	2	3	3	3	3
Kazakhstan	0	0	2	2	1	2	0	0	0	0
Malaysia	3	3	3	3	3	3	3	3	3	3
Brunei	3	2	2	1	2	3	3	3	3	3
P.R. China	2	2	2	2	3	2	3	2	2	2
Mongolia	1	2	2	1	1	2	1	2	2	1
Uzbekistan	2	2	3	2	2	2	3	2	2	1
Bhutan	0	0	1	0	1	1	1	0	0	0
Samoa	1	1	2	2	2	2	1	0	0	0
Nepal	0	0	1	0	0	2	1	1	1	0
Lao PDR	0	0	0	0	0	0	0	0	0	0
Solomon Islands	0	0	1	0	0	0	0	0	0	0
Bangladesh	1	1	3	1	2	3	3	2	2	0
Afghanistan	1	1	1	0	0	1	1	1	0	1
Niue	0	0	1	1	3	2	0	0	0	1
Micronesia	0	0	0	0	0	0	0	0	0	0
Palau	0	0	1	2	2	1	0	0	0	0
Cook Islands	0	0	1	0	1	0	0	0	0	0

Category: Education

Sub-group : Education policies targeting caregivers (0-8 years old age group)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	2.1.1 Ministry of Education has policies / programmes / resources targeting caregivers (parents, guardians, teachers) that promote...							
	...guidance on posting information (how much, what type) about children.	...securing personal, school, and family data.	...training for teachers and school ICT staff on use of ICT provisions in school.	...appropriate adult mediation on children's ICT use through the use of content filtering services.	...appropriate adult mediation on children's ICT use through guidance on healthy limits of screen time.	...appropriate adult mediation on children's ICT use in prevention and intervention for pornography, gaming, and other addictive behaviour.	...national standards for teacher preparation that include ICT literacy skills, cyber wellness and cyber security skills and competencies.	...faculty development programmes on ICT use for learning that include cyber wellness and cyber security components.
Korea (Rep.)	0	0	0	0	2	2	0	0
Japan	0	0		2	2	2		2
Australia	2	2	2	2	1	2	0	0
New Zealand	2	3	3	2	2	2	0	0
Singapore	NR	NR	NR	NR	NR	NR	NR	NR
Kazakhstan	0	0	0	0	0	0	0	0
Malaysia	3	3	3	3	3	3	3	3
Brunei	3	3	3	3	3	3	3	3
P.R. China	2	2	3	3	2	2	2	2
Mongolia	2	2	2	1	1	1	1	1
Uzbekistan	2	2	3	2	1	2	3	2
Bhutan	0	0	0	0	0	0	0	0
Samoa	0	0	0	0	0	0	0	2
Nepal	0	0	0	0	0	0	0	0
Lao PDR	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0
Bangladesh	2	0	1	2	1	0	2	2
Afghanistan	0	1	2	2	0	2	1	1
Niue	1	2	2	2	2	0	2	0
Micronesia	0	0	0	0	0	0	0	0
Palau	2	2	2	0	0	0	0	2
Cook Islands	1	1	2	2	0	0	0	1

Category: Education

Sub-group: Education policies targeting caregivers (9-12 years old age group)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	2.2.1 Ministry of Education has policies / programmes / resources targeting caregivers (parents, guardians, teachers) that promote...							
	...guidance on posting information (how much, what type) about children.	...securing personal, school, and family data.	...training for teachers and school ICT staff on use of ICT provisions in school.	...appropriate adult mediation on children's ICT use through the use of content filtering services.	...appropriate adult mediation on children's ICT use through guidance on healthy limits of screen time.	...appropriate adult mediation on children's ICT use in prevention and intervention for pornography, gaming, and other addictive behaviour.	...national standards for teacher preparation that include ICT literacy skills, cyber wellness and cyber security skills and competencies.	...faculty development programmes on ICT use for learning that include cyber wellness and cyber security components.
Korea (Rep.)	3	3	3	0	2	2	0	2
Japan	0	0	NR	2	2	2	NR	2
Australia	2	2	2	2	1	2	1	1
New Zealand	2	3	2	2	2	2	0	0
Singapore	3	3	2	3	2	2	2	2
Kazakhstan	0	0	0	0	0	0	0	0
Malaysia	3	3	3	3	3	3	3	3
Brunei	3	3	3	3	3	3	3	3
P.R. China	2	2	3	2	2	2	2	2
Mongolia	1	2	2	2	1	1	1	1
Uzbekistan	2	2	2	2	1	2	3	1
Bhutan	1	1	1	1	1	1	1	1
Samoa	2	2	2	0	0	0	2	2
Nepal	2	2	2	0	0	0	0	0
Lao PDR	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0
Bangladesh	1	2	2	2	2	0	0	2
Afghanistan	0	1	2	3	3	3	1	1
Niue	2	2	2	2	0	0	2	0
Micronesia	0	0	0	0	0	0	0	0
Palau	0	2	0	0	0	0	0	0
Cook Islands	0	0	2	2	0	0	0	0

Category: Education

Sub-group: Education policies targeting caregivers (13-18 years old age group)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	2.3.1 Ministry of Education has policies / programmes / resources targeting caregivers (parents, guardians, teachers) that promote...							
	...guidance on posting information (how much, what type) about children.	...securing personal, school, and family data.	...training for teachers and school ICT staff on use of ICT provisions in school.	...appropriate adult mediation on children's ICT use through the use of content filtering services.	...appropriate adult mediation on children's ICT use through guidance on healthy limits of screen time.	...appropriate adult mediation on children's ICT use in preventionand intervention for pornography, gaming, and other addictive behaviour.	...national standards for teacher preparation that include ICT literacy skills, cyber wellness and cyber security skills and competencies.	...faculty development programmes on ICT use for learning that include cyber wellness and cyber security components.
Korea (Rep.)	3	3	3	0	2	2	0	2
Japan	0	0	NR	2	2	2	NR	2
Australia	2	2	2	2	1	2	1	1
New Zealand	2	2	2	2	1	1	2	2
Singapore	3	3	3	3	3	3	3	3
Kazakhstan	0	0	0	0	0	0	0	0
Malaysia	3	3	3	3	3	3	3	3
Brunei	3	3	3	3	3	3	3	3
P.R. China	2	2	3	2	2	2	3	2
Mongolia	1	2	2	1	1	1	1	1
Uzbekistan	2	2	2	2	2	2	2	2
Bhutan	1	1	1	1	1	1	2	1
Samoa	2	2	2	2	0	0	2	2
Nepal	2	2	2	0	0	0	0	0
Lao PDR	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0
Bangladesh	2	2	2	2	2	2	2	2
Afghanistan	1	1	1	1	0	0	0	0
Niue	0	0	0	0	0	0	0	0
Micronesia	0	0	0	0	0	0	0	0
Palau	0	0	0	0	0	0	0	0
Cook Islands	0	1	1	3	0	0	0	0

Education policies targeting students (0-8 years old age group)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	2.1.2. Ministry of Education has policies / programmes / resources targeting students that promote...								
	...basic ICT literacy skills.	...digital storytelling, computer coding, and production of other ICT outputs.	...healthy limits of screen time / healthy balance between online and offline activities.	...building and maintaining a positive digital reputation.	...privacy skills and competencies.	...cyber security skills and competencies.	...creating, communicating and collaborating online / safe and responsible social networking, including content viewing and sharing.	...ethical use of creative content (content owned by others).	...appropriate response to cyber-bullying.
Korea (Rep.)	0	0	0	0	0	0	0	0	0
Japan	3	2	2	NR	2	2	2	2	2
Australia	2	0	1	1	2	2	0	1	2
New Zealand	3	2	2	2	2	2	2	2	2
Singapore	NR	NR	NR	NR	NR	NR	NR	NR	NR
Kazakhstan	1	1	0	0	0	0	0	0	0
Malaysia	2	2	2	2	2	2	2	2	2
Brunei	3	3	3	3	2	2	2	2	3
P.R. China	3	2	1	1	2	1	3	3	3
Mongolia	1	1	0	1	1	1	1	2	2
Uzbekistan	3	2	1	2	1	1	1	1	1
Bhutan	0	0	0	0	0	0	0	0	0
Samoa	0	0	0	0	0	0	0	0	0
Nepal	0	0	0	0	0	0	0	0	0
Lao PDR	0	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0	0
Bangladesh	2	2	2	1	2	2	2	1	2
Afghanistan	2	0	2	1	0	0	2	1	0
Niue	3	2	0	2	2	2	2	2	0
Micronesia	0	0	0	0	0	0	0	0	0
Palau	0	0	0	0	0	0	0	0	0
Cook Islands	2	2	0	0	0	0	0	0	0

Category: Education

Sub-group: Education policies targeting students (9-12 years old age group)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	2.2.2. Ministry of Education has policies / programmes / resources targeting students that promote...								
	...basic ICT literacy skills.	...digital storytelling, computer coding, and production of other ICT outputs.	...healthy limits of screen time / healthy balance between online and offline activities.	...building and maintaining a positive digital reputation.	...privacy skills and competencies.	...cyber security skills and competencies.	...creating, communicating and collaborating online / safe and responsible social networking, including content viewing and sharing.	...ethical use of creative content (content owned by others).	...appropriate response to cyber-bullying.
Korea (Rep.)	3	2	0	2	2	2	2	2	2
Japan	3	2	2	NR	2	2	2	2	2
Australia	2	1	2	2	2	2	2	2	2
New Zealand	NR	NR	NR	NR	NR	NR	NR	NR	NR
Singapore	3	3	3	3	3	3	3	3	3
Kazakhstan	1	0	0	0	0	0	0	0	0
Malaysia	3	3	3	3	3	3	3	3	3
Brunei	3	3	3	3	3	3	3	3	2
P.R. China	3	2	1	1	2	2	2	2	2
Mongolia	1	1	1	1	1	1	1	1	1
Uzbekistan	3	2	1	2	1	1	1	1	1
Bhutan	1	1	1	1	1	1	1	1	1
Samoa	0	0	0	0	0	0	0	0	0
Nepal	2	1	0	0	0	1	1	0	0
Lao PDR	0	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0	0
Bangladesh	2	2	2	2	2	1	2	2	2
Afghanistan	2	0	2	3	2	0	2	2	0
Niue	2	0	0	0	0	0	0	0	0
Micronesia	0	0	0	0	0	0	0	0	0
Palau	0	0	0	0	0	0	0	0	0
Cook Islands	2	2	0	0	0	0	0	0	0

Category: Education

Sub-group: Education policies targeting students (13-18 years old age group)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	2.3.2. Ministry of Education has policies / programmes / resources targeting students that promote...								
	...basic ICT literacy skills.	...digital storytelling, computer coding, and production of other ICT outputs.	...healthy limits of screen time / healthy balance between online and offline activities.	...building and maintaining a positive digital reputation.	...privacy skills and competencies.	...cyber security skills and competencies.	...creating, communicating and collaborating online / safe and responsible social networking, including content viewing and sharing.	...ethical use of creative content (content owned by others).	...appropriate response to cyber-bullying.
Korea (Rep.)	3	2	0	2	2	2	2	2	2
Japan	3	2	2	NR	2	2	2	2	2
Australia	2	1	1	2	2	2	2	1	2
New Zealand	3	3	1	2	2	2	2	2	2
Singapore	3	3	3	3	3	3	3	3	3
Kazakhstan	1	0	0	0	0	0	0	0	0
Malaysia	3	3	3	3	3	3	3	3	3
Brunei	3	3	3	3	3	3	3	3	3
P.R. China	3	2	2	2	3	2	2	2	2
Mongolia	2	1	1	1	1	1	1	1	1
Uzbekistan	3	2	1	2	1	1	1	1	1
Bhutan	2	2	2	2	2	2	2	2	2
Samoa	2	0	0	2	2	2	2	2	2
Nepal	2	1	0	0	0	0	0	0	0
Lao PDR	0	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0	0
Bangladesh	2	2	2	2	2	1	2	2	2
Afghanistan	2	0	0	0	0	0	0	0	0
Niue	3	0	0	2	2	2	3	0	2
Micronesia	0	0	0	0	0	0	0	0	0
Palau	0	0	0	0	0	0	0	0	0
Cook Islands	3	2	0	0	0	0	0	1	0

Category: Education

Sub-group: Education policies targeting individual schools (0-8 years old)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	2.1.3 Ministry of Education has policies / programmes / resources targeting individual schools that promote...										
	..."lifelong learning" activities with digital-age learning tools and content.	...use of student-owned devices.	...integrating innovative ICT-supported learning initiatives into curricular activities.	...incorporating safe and responsible use of ICT / cyber wellness in the curriculum.	...incorporating safe and responsible use of ICT / cyber wellness in co-curricular or extracurricular activities.	...use and publication of digital and video images.	...use of Acceptable Use Policies (AUP) by school stakeholders.	...Acceptable Use Policies (AUP) that include sanctions for ICT abuse and misuse.	...formation of multi-stakeholder cyber wellness committees.	...conduct of safe and responsible use of ICT / cyber wellness sessions with caregivers.	...prevention and intervention for pornography, gaming, and other addictive behaviour.
Korea (Rep.)	0	0	0	0	0	0	0	0	0	0	0
Japan	2	2	2	2	2	NR	2	NR	NR	NR	2
Australia	0	2	1	1	0	1	2	2	0	1	2
New Zealand	2	2	2	2	2	2	2	2	2	3	2
Singapore	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR
Kazakhstan	0	0	0	0	0	0	0	0	0	0	0
Malaysia	2	0	3	3	3	3	3	3	3	3	3
Brunei	3	2	3	3	3	3	3	3	3	3	3
P.R. China	2	2	3	2	3	2	2	2	2	2	2
Mongolia	2	2	1	2	2	2	1	1	1	1	1
Uzbekistan	2	2	3	1	1	1	1	1	1	1	2
Bhutan	0	0	1	0	0	1	0	0	0	0	0
Samoa	0	0	0	0	0	0	0	0	0	0	0
Nepal	0	0	0	0	0	0	0	0	0	0	0
Lao PDR	0	0	0	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0	0	0	0
Bangladesh	2	1	2	2	2	2	2	2	2	2	1
Afghanistan	2	1	3	0	0	3	1	1	0	0	3
Niue	2	0	0	0	0	0	2	2	0	0	0
Micronesia	0	0	0	0	0	0	0	0	0	0	0
Palau	0	0	0	0	0	0	0	0	0	0	0
Cook Islands	2	2	2	0	0	0	3	3	0	0	0

Category: Education

Sub-group: Education policies targeting individual schools (9-12 years old)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	2.2.3 Ministry of Education has policies / programmes / resources targeting individual schools that promote...										
	..."lifelong learning" activities with digital-age learning tools and content.	...use of student-owned devices.	...integrating innovative ICT-supported learning initiatives into curricular activities.	...incorporating safe and responsible use of ICT / cyber wellness in the curriculum.	...incorporating safe and responsible use of ICT / cyber wellness in co-curricular or extracurricular activities.	...use and publication of digital and video images.	...use of Acceptable Use Policies (AUP) by school stakeholders.	...Acceptable Use Policies (AUP) that include sanctions for ICT abuse and misuse.	...formation of multi-stakeholder cyber wellness committees.	...conduct of safe and responsible use of ICT / cyber wellness sessions with caregivers.	...prevention and intervention for pornography, gaming, and other addictive behaviour.
Korea (Rep.)	3	0	3	3	3	2	0	0	0	0	3
Japan	2	2	2	2	2	NR	2	NR	NR	NR	2
Australia	0	2	1	2	2	2	2	2	0	2	2
New Zealand	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR
Singapore	3	3	3	3	3	3	2	2	3	3	3
Kazakhstan	0	0	0	0	0	0	0	0	0	0	0
Malaysia	3	3	3	3	3	3	3	3	3	3	3
Brunei	3	3	3	3	3	3	3	3	3	3	3
P.R. China	2	2	3	3	3	2	2	2	2	2	2
Mongolia	1	1	1	1	1	2	2	2	1	1	1
Uzbekistan	2	2	3	2	2	2	2	2	2	2	2
Bhutan	0	0	1	1	0	0	0	1	0	0	1
Samoa	0	0	0	0	0	0	0	0	0	0	0
Nepal	1	0	1	0	0	1	0	0	0	0	0
Lao PDR	0	0	0	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0	0	0	0
Bangladesh	1	1	2	2	2	2	2	2	2	2	1
Afghanistan	2	1	2	0	0	2	2	1	0	0	2
Niue	2	0	0	0	0	0	0	0	0	0	0
Micronesia	0	0	0	0	0	0	0	0	0	0	0
Palau	0	2	0	0	0	0	0	0	0	0	0
Cook Islands	2	2	2	0	0	0	3	3	0	0	0

Category: Education

Sub-group: Education policies targeting individual schools (13-18 years old age group)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	2.3.3 Ministry of Education has policies / programmes / resources targeting individual schools that promote...										
	..."lifelong learning" activities with digital-age learning tools and content.	...use of student-owned devices.	...integrating innovative ICT-supported learning initiatives into curricular activities.	...incorporating safe and responsible use of ICT / cyber wellness in the curriculum.	...incorporating safe and responsible use of ICT / cyber wellness in co-curricular or extracurricular activities.	...use and publication of digital and video images.	...use of Acceptable Use Policies (AUP) by school stakeholders.	...Acceptable Use Policies (AUP) that include sanctions for ICT abuse and misuse.	...formation of multi-stakeholder cyber wellness committees.	...conduct of safe and responsible use of ICT / cyber wellness sessions with caregivers.	...prevention and intervention for pornography, gaming, and other addictive behaviour.
Korea (Rep.)	3	0	3	3	3	2	0	0	0	0	3
Japan	2	2	2	2	2	NR	2	NR	NR	NR	2
Australia	0	2	1	2	1	1	2	2	0	2	2
New Zealand	2	2	2	2	2	2	2	2	2	2	1
Singapore	3	3	3	3	3	3	2	2	3	3	3
Kazakhstan	0	0	0	0	0	0	0	0	0	0	0
Malaysia	3	3	3	3	3	3	3	3	3	3	3
Brunei	3	3	3	3	3	3	3	3	3	3	NR
P.R. China	2	3	3	3	3	2	2	2	2	2	2
Mongolia	2	1	2	1	1	2	2	1	1	1	1
Uzbekistan	2	2	3	2	2	2	2	2	2	2	2
Bhutan	0	0	1	1	0	0	0	1	0	0	1
Samoa	2	1	2	2	2	2	2	0	NR	2	2
Nepal	1	0	1	0	0	0	0	0	0	0	0
Lao PDR	0	0	0	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0	0	0	0
Bangladesh	2	2	2	2	2	2	2	2	2	2	1
Afghanistan	0	0	1	1	1	1	1	0	0	0	0
Niue	3	0	0	3	2	2	2	2	2	2	2
Micronesia	0	0	0	0	0	0	0	0	0	0	0
Palau	0	0	0	0	0	0	0	0	0	0	0
Cook Islands	2	1	1	0	0	1	3	3	0	0	0

Category: Technical infrastructure (0-8 years old age group)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	3.1 Please answer with respect to early childhood to early primary school level (i.e. children from 0 to 8 years old)								
	Schools provide at least the minimum number of computers per school (e.g. computer: student ratio is greater than one computer lab per school).	School's minimum bandwidth requirement is set at the national level.	Schools use cloud services.	Schools use secured wifi.	Schools use secured networks.	Schools use secured encryption.	Schools regularly review and audit the safety and security of school ICT systems with oversight from senior leaders.	Schools augment internal reviews with rigorous external reviews of the security of school systems.	Budgets support ICT technical personnel for schools to ensure policies are observed.
Korea (Rep.)	0	0	0	2	2	2	2	2	0
Japan	2	NR	2	2	2	2	2	NR	2
Australia	2	0	0	2	2	2	0	0	1
New Zealand	0	0	0	0	0	0	0	0	0
Singapore	NR	NR	NR	NR	NR	NR	NR	NR	NR
Kazakhstan	2	2	0	1	1	1	0	0	1
Malaysia	3	3	3	3	3	3	3	3	3
Brunei	3	3	3	3	3	3	2	2	2
P.R. China	3	3	2	2	3	2	2	2	2
Mongolia	1	1	0	0	0	0	0	0	0
Uzbekistan	2	2	1	1	3	1	1	1	1
Bhutan	0	0	0	0	0	0	0	0	0
Samoa	0	0	0	0	0	0	0	0	0
Nepal	0	0	0	0	0	0	0	0	0
Lao PDR	0	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0	0
Bangladesh	0	1	1	1	1	1	0	1	2
Afghanistan	0	0	0	0	0	0	0	0	0
Niue	1	1	0	1	1	1	1	1	1
Micronesia	0	0	0	0	0	0	0	0	0
Palau	2	0	0	0	0	0	0	0	0
Cook Islands	3	0	0	0	0	0	0	0	0

Category: Technical infrastructure (9-12 years old age group)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	3.2 Please answer with respect to primary school level (i.e. children from 9 to 12 years old).								
	Schools provide at least the minimum number of computers per school (e.g. computer: student ratio is greater than one computer lab per school).	School's minimum bandwidth requirement is set at the national level.	Schools use cloud services.	Schools use secured wifi.	Schools use secured networks.	Schools use secured encryption.	Schools regularly review and audit the safety and security of school ICT systems with oversight from senior leaders.	Schools augment internal reviews with rigorous external reviews of the security of school systems.	Budgets support ICT technical personnel for schools to ensure policies are observed.
Korea (Rep.)	0	0	2	2	2	2	2	2	0
Japan	2	NR	2	2	2	2	2	NR	2
Australia	2	0	0	2	2	2	0	0	1
New Zealand	2	3	2	2	2	2	2	1	1
Singapore	NR	NR	NR	NR	NR	NR	NR	NR	NR
Kazakhstan	2	2	0	1	1	1	0	0	1
Malaysia	3	3	3	3	3	3	3	3	3
Brunei	3	3	3	3	3	3	2	2	2
P.R. China	2	3	2	2	3	2	2	1	1
Mongolia	1	1	0	0	0	0	0	0	0
Uzbekistan	3	2	2	2	3	1	2	2	1
Bhutan	1	1	0	0	0	0	0	0	0
Samoa	0	0	0	0	0	0	0	0	0
Nepal	2	2	0	0	0	0	0	0	0
Lao PDR	0	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0	0
Bangladesh	2	2	2	0	1	2	1	1	1
Afghanistan	0	0	0	0	0	0	0	0	0
Niue	1	1	0	1	1	1	1	1	1
Micronesia	0	0	0	0	0	0	0	0	0
Palau	2	0	0	0	0	0	0	0	0
Cook Islands	3	0	0	0	0	0	0	0	0

Category: Technical infrastructure (13-18 years old)

Legend:

Level 0: No policy is in place

Level 1: There is a policy, but it is not implemented

Level 2: There is a policy that is implemented (budget/resources are provided)

Level 3: There is a policy that is implemented and monitored/evaluated

NR = No Response, i.e. not included in the statistical analysis

What country do you represent?	3.3 Please answer with respect to secondary school level (i.e. children from 13 to 18 years old).								
	Schools provide at least the minimum number of computers per school (e.g. computer: student ratio is greater than one computer lab per school).	School's minimum bandwidth requirement is set at the national level.	Schools use cloud services.	Schools use secured wifi.	Schools use secured networks.	Schools use secured encryption.	Schools regularly review and audit the safety and security of school ICT systems with oversight from senior leaders.	Schools augment internal reviews with rigorous external reviews of the security of school systems.	Budgets support ICT technical personnel for schools to ensure policies are observed.
Korea (Rep.)	0	0	2	2	2	2	2	2	0
Japan	2	NR	2	2	2	2	2	NR	2
Australia	2	0	0	2	2	2	0	0	1
New Zealand	2	3	2	2	2	2	2	1	1
Singapore	NR	NR	NR	NR	NR	NR	NR	NR	NR
Kazakhstan	2	2	0	1	1	1	0	0	1
Malaysia	3	3	3	3	3	3	3	3	3
Brunei	3	3	3	3	3	3	2	2	2
P.R. China	2	3	2	2	3	2	2	2	2
Mongolia	1	1	0	0	0	0	0	0	0
Uzbekistan	3	2	2	2	3	2	2	2	1
Bhutan	2	1	0	0	0	0	0	0	0
Samoa	2	0	0	2	2	0	0	0	0
Nepal	2	2	0	0	0	0	0	0	0
Lao PDR	0	0	0	0	0	0	0	0	0
Solomon Islands	0	0	0	0	0	0	0	0	3
Bangladesh	1	2	1	1	1	2	1	1	2
Afghanistan	1	0	0	0	0	0	0	0	0
Niue	3	3	3	3	3	3	3	3	3
Micronesia	0	0	0	0	0	0	0	0	0
Palau	2	0	0	0	0	0	0	0	0
Cook Islands	3	0	0	0	0	0	0	0	0

Category: Technical infrastructure

Open-ended responses

NR = No Response

What country do you represent?	3.4 Has a National Educational Management Information System (EMIS) been established?	3.5 If so, how long has the EMIS been in place?	3.6 Does the EMIS include acquisition of information on cyber safety?	3.7 Have content filtering and/or monitoring systems been established? (please check ALL that apply: No, National level, Provincial level, Local level)				3.8 Are school-based ICT systems audited for safety and security? (please check the ONE that best matches your system)	3.9 Has an agency been established to review products and services for security and safety before products can be used in schools?	3.10 If yes, please identify agency:	3.11 Is a national-level mechanism in place to monitor ICT utilisation rate in schools?	3.12 If yes, is this information shared with school leaders? (please check ALL that apply)	3.13 Is a national-level system in place to assess effective pedagogical practices in the use of ICT in schools?	3.14 If yes, is this information shared with school leaders? (please check ALL that apply)
Open-Ended Response	Response	Response	Response	No	Yes	Yes	Yes	Response	Response	Open-Ended Response	Response	Response	Response	Response
Korea (Rep.)	Yes	Longer than ten years	N/A		Yes	Yes		Yes, monthly	Yes	Provincial Education Office	Yes	N/A	Yes	Yes, with local school leaders
Japan	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR	Yes	Yes, with local school leaders	Yes	Yes, with provincial school leaders
Australia	No	N/A	N/A	NR	NR	Yes	Yes	Yes, weekly	No	NR	No	N/A	No	N/A
New Zealand	No	N/A	N/A	NR	Yes			No	No	NR	Yes	Yes, with provincial leaders	No	
Singapore	Yes	N/A	Yes	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR
Kazakhstan	Yes	Five years	No	NR	NR		Yes	No	No	NR	No	N/A	No	N/A
Malaysia	Yes	Longer than ten years	Yes	NR	Yes	Yes	Yes	Yes, quarterly	Yes	NR	Yes	Yes, with local school leaders	Yes	Yes, with local school leaders
Brunei	Yes	Ten years	Yes	NR	Yes	Yes	Yes	Yes, quarterly	Yes	ICT Department, Curriculum Department, Media and in Service Centre	Yes	Yes, with provincial leaders	No	N/A
P.R.China	Yes	Five years	Yes	NR	NR	NR	Yes	Yes, annually	No	NR	No	NR	Yes	N/A
Mongolia	Yes	N/A	Yes	NR	Yes	NR	NR	Yes, annually	No	NR	No	NR	No	
Uzbekistan	Yes	Ten years	No	NR	Yes	NR	NR	Yes, quarterly	Yes	Center of the development of multimedium general education programmes	Yes	Yes, with local school leaders	Yes	Yes, with local school leaders

What country do you represent?	3.4 Has a National Educational Management Information System (EMIS) been established?	3.5 If so, how long has the EMIS been in place?	3.6 Does the EMIS include acquisition of information on cyber safety?	3.7 Have content filtering and/or monitoring systems been established? (please check ALL that apply: No, National level, Provincial level, Local level)				3.8 Are school-based ICT systems audited for safety and security? (please check the ONE that best matches your system)	3.9 Has an agency been established to review products and services for security and safety before products can be used in schools?	3.10 If yes, please identify agency:	3.11 Is a national-level mechanism in place to monitor ICT utilisation rate in schools?	3.12 If yes, is this information shared with school leaders? (please check ALL that apply)	3.13 Is a national-level system in place to assess effective pedagogical practices in the use of ICT in schools?	3.14 If yes, is this information shared with school leaders? (please check ALL that apply)
Open-Ended Response	Response	Response	Response	No	Yes	Yes	Yes	Response	Response	Open-Ended Response	Response	Response	Response	Response
Bhutan	Yes	Five years	No	NR	Yes	Yes	Yes	No	Yes	Department of Information Technology & Telecom, Ministry of Information & Communications, Bhutan	No	NR	NR	NR
Samoa	Yes	Five years	No	NR	Yes	NR	NR	No	No	NR	No	NR	No	NR
Nepal	Yes	Longer than ten years	No	No	NR	NR	NR	No	Yes	Department of Education	No	NR	No	NR
Lao PDR	Yes	N/A	N/A	No	NR	NR	NR	No	No	NR	No	N/A	No	N/A
Solomon Islands	Yes	N/A	No	NR	NR	NR	Yes	No	No	Solomon Islands Government has established its own ICT Unit via Ministry of Finance but this is for central government departments use only thus far.	No	N/A	No	N/A
Bangladesh	Yes	Longer than ten years	Yes	NR	Yes	NR	Yes	No	No	NR	Yes	Yes, with local school leaders	Yes	Yes, with local school leaders
Afghanistan	Yes	Five years	No	NR	Yes	NR		No	No	NR	No	NR	No	NR
Niue	Yes	Five years	Yes	NR		NR	Yes	Yes, daily	Yes	NZQA, Niue delivers the NZ Curriculum	No	N/A	No	N/A
Micronesia	Yes	Five years	No	NR	Yes	NR	NR	No	No	NR	No	NR	No	NR
Palau	No	N/A	N/A	No	NR	NR	NR	No	No	NR	No	N/A	No	N/A
Cook Islands	Yes	Longer than ten years	No	NR	Yes	Yes	Yes	Yes, weekly	No	NR	Yes	Yes, with local school leaders	Yes	Yes, with local school leaders

Appendix 4. Categorization of policy orientations

Opportunity-oriented policies	Safety- and risk-oriented policies
...training for teachers and school ICT staff on use of ICT provisions in school.	...guidance on posting information (how much, what type) about children.
...faculty development programmes on ICT use for learning that include cyber wellness and cyber security components.	...securing personal, school, and family data.
...ethical use of creative content (content owned by others).	....appropriate adult mediation on children's ICT use through the use of content filtering services
...national standards for teacher preparation that include ICT literacy skills, cyber wellness and cyber security skills and competencies.	...appropriate adult mediation on children's ICT use through guidance on healthy limits of screen time.
...basic ICT literacy skills.	...appropriate adult mediation on children's ICT use in prevention and intervention for pornography, gaming, and other addictive behaviour.
...digital storytelling, computer coding, and production of other ICT outputs.	...healthy limits of screen time / healthy balance between online and offline activities.
...building and maintaining a positive digital reputation.	...privacy skills and competencies.
...creating, communicating and collaborating online / safe and responsible social networking, including content viewing and sharing.	...cyber security skills and competencies.
..."lifelong learning" activities with digital-age learning tools and content.	...appropriate response to cyber-bullying.
...use of student-owned devices.	...incorporating safe and responsible use of ICT / Cyber Wellness in the curriculum.

Opportunity-oriented policies	Safety- and risk-oriented policies
...integrating innovative ICT-supported learning initiatives into curricular activities.	...incorporating safe and responsible use of ICT / Cyber Wellness in co-curricular or extracurricular activities.
...use and publication of digital and video images.	...use of Acceptable Use Policies (AUP) by school stakeholders.
	...Acceptable Use Policies (AUP) that include sanctions for ICT abuse and misuse.
	...conduct of safe and responsible use of ICT / Cyber Wellness sessions with caregivers.
	...prevention and intervention for pornography, gaming, and other addictive behaviour.

UNESCO Bangkok Office
Asia and Pacific Regional Bureau for Education
Mom Luang Pin Malakul Centenary Building
920 Sukhumvit Road, Prakanong, Klongtoei
Bangkok 10110, Thailand
Email: ict.bgk@unesco.org
Website: www.unesco.org/bangkok
Tel: +66-2-3910577 Fax: +66-2-3910866