

Child Online Protection in Rwanda

Child Online Protection in Rwanda

Professor Julia Davidson
Baroness Beeban Kidron
Kirsty Phillips

5Rights Foundation, University of East London,
In collaboration with The University Of Rwanda.
On behalf of the Ministry of ICT and Innovation,
Government of Rwanda.



5Rights
FOUNDATION



University of
East London



UNIVERSITY of
RWANDA

This work was supported by End Violence Against Children, The Fund [18-evac-0029-University of East London]



FOREWORD

The invitation from the Rwandan Government to create a Child Online Protection Policy was a singular opportunity to consider how to conceive protection in a dynamic and changing technological world.

Rwanda has set its sights on being a connected nation, it has prioritised investment in developing skills and innovation and it has collaborated with the international community to make sure, as digital emerges as the new norm in the way a society operates, that Rwanda is front and centre of that change.

Child Online Protection is something that all nations struggle with equally. The rapid growth of a technology that did not at the outset envisage that it would be an environment in which childhood would take place, the network effect that super-charged communication, the domination of a handful of companies that developed a corporate model that relies on data gathering and profiling created an environment in which children need specific protections.

Digital technology does not have one responsible stakeholder, it has many. From governments, regulators, international institutions and the enforcement community – to civil society, business, the tech sector, academia, teachers, families, parents, even children themselves. Child Online Protection relies on all of these stakeholders working in partnership, each taking their part of that responsibility, each doing what is necessary to protect children.

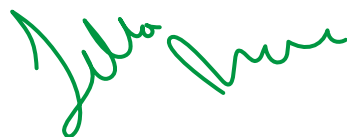
The Child Online Protection Policy set out in this report offers the opportunity for all to play their part.

Created in partnership between 5Rights Foundation, University of East London, University of Rwanda and the Government of Rwanda, it has benefited from input from a remarkable range of experts. The resulting policy and its high-level implementation plan offer an exemplar for any nation considering Child Online Protection.

We would like to extend our thanks to all those who gave their time, their expertise, told their stories and who supported our work in multiple ways. We owe special thanks to the Government of Rwanda for trusting us with this work, our funders End Violence Against Children, and our colleagues at 5Rights Foundation and UEL who supported this endeavour particularly Project Coordinator Kirsty Phillips.

As we go to press, it was announced that the Government of Rwanda's Cabinet formally adopted the Child Online Protection Policy, listed as number 1 of approved policies¹ with the Ministry of ICT & Innovation (MINICT)², which represents a step-change for the children of Rwanda.

Children are essential for any nation's development and flourishing – to invest in their safety, and allow them to access the digital environment creatively, knowledgeably and fearlessly, is to invest in the future.



Professor Julia Davidson



Baroness Beeban Kidron

¹ https://minict.gov.rw/fileadmin/Documents/Policies2019/COP_Policy_Updated.pdf

² <https://www.minict.gov.rw/>

TABLE OF CONTENTS

| | |
|--|----|
| The Rwandan Context | 1 |
| Project Aims and Objectives | |
| The Rwandan Context | |
| Respondent Interviews | |
| Child Online Protection Policy Document | 16 |
| Child Online Protection Five-Year Implementation Plan | 28 |
| Child Online Protection Communications | 32 |
| Conclusion | 42 |
| Contributors | 44 |
| Further Resources | 52 |
| Resource Directory COP Policy Document | |
| Institutional Capacity | |
| Legal and Regulatory | |
| COP Response Systems | |
| Technical Controls and Corporate Responsibility | |
| Education | |
| Public Awareness | |
| Research and Development | |
| Appendix | |
| A. COP Organisations | |
| B. COP Module Outline for Teachers & Educators | |
| C. Terminology Guidelines for COP | |
| D. Report on Government of Rwanda visit to Police Scotland | |
| E. A Review of Online Child Protection Laws in Rwanda | |
| F. Data Protection Regulation Recommendation | |
| G. Further reading on the Rwandan Context | |

The Rwandan Context

Project Aims and Objectives

Rwanda is committed to the roll out of ICT technology and ensuring that children and adolescents benefit from it. Rwanda is a regional leader in embracing digital innovation under the leadership of His Excellency Paul Kagame, President of the Republic of Rwanda, Vice-Chair of the Broadband Commission for Sustainable Development. It is in this positive context that Rwanda wished to develop a Child Online Protection (COP) policy.

In early 2018 Baroness Beeban Kidron, Founder and Chair of 5Rights Foundation, met with the Minister for ICT and discussed some of the underlying issues that compromise effective COP policy development, across all jurisdictions. They include (but are not limited to):

- Acceptance of the problem;
- Definition of terms;
- Institutional capacity;
- Understanding the breadth and nature of COP issues;
- The presence of Data regulation;
- Training (at all levels including judiciary, enforcement, policy, education, children's services);
- Effective cross-sectorial coordination and leadership;
- Resources both human and financial;
- Mechanisms to capture the voice of children;
- Commercial drivers;
- Institutional and public messaging.

To support the Government of Rwanda in COP implementation, Professor Julia Davidson of University of East London and Baroness Beeban Kidron, Chair of 5Rights Foundation, undertook to develop a National Child Online Protection Policy and Implementation Plan on behalf of the Government of Rwanda.

This project aims and this report involves the following components:

- A literature review identifying information relevant to the Rwandan context in relation to the internet, ICT and COP
- A research study based on respondent interviews, to establish capability gaps in relation to COP in Rwanda
- Production of a Child Online Protection policy based on international best practice, and in consultation with a cross-sector expert working group (established as part of the project) and the Government of Rwanda
- Production of a Five-Year Implementation Programme based on international best practice, and in consultation with a cross-sector expert working group and the Government of Rwanda
- Key resources to assist in enacting the policy and the implementation plan, including working with the Government of Rwanda to build institutional knowledge and capacity;
- Development of a communications strategy for the roll out of a COP public awareness campaign

The Rwandan Context

The Internet is a global phenomenon. Whilst the safe and creative use of Digital Technologies offer children previously unimaginable opportunities, there is a growing understanding of the risks and harms associated with its use, and the possibility of designing digital systems to support beneficial outcomes for children. Children in the global North are disproportionately higher internet users, compared to other age groups (Bulger, Burton, O'Neill, & Staksrud, 2017). Their access to and use of ICT devices, their experience of harms, and the impacts of internet use has been intensely investigated. These same quantities, however, are relatively unknown for children in the global South. Research on children's internet use in Africa is still in its infancy and at present only a small body of literature exists. The area that has most intensely studied is South Africa, and only a few studies have been identified in other areas (namely; Nigeria, Tanzania, Ethiopia, Zimbabwe and Ghana). Some of the recommendations in the policy and implementation plan come from these broader regional and international contexts.

Additionally, more specific legislation relating to child protection has been developed in the global North (Phyfer, Burton, & Leoschut, 2016). And yet, given the fast pace and ever-changing online environment, further reforms are required in all jurisdictions, as evidenced, for example, by the recently published and world-leading UK government White Paper on Online Harms³ (April 2019) and the Information Commissioner's Office Age Appropriate Design Code⁴ (April 2019). It is increasingly evident that nation states are acting to ensure that children's rights and privileges are protected equally in both offline and online environments and that services providers will in future be subject to greater regulation. It is anticipated that there will be an upsurge in the number of young people who access the Internet in developing countries (Bulger, Burton, O'Neill, & Staksrud, 2017). This rapid online expansion means that "an urgent shift in attention towards conditions of access faced by children in developing countries may be required" (p.754).

Rwanda is experiencing a rapid increase in connectivity and use of digital devices. The digital environment is universal, and digital use and COP do not occur in a vacuum. To ensure that the Government's online Policy was evidence based and appropriate for the Rwandan context, a research gap analysis was conducted. Broad social context and emergent issues were considered, along with an overview of the Rwandan context in relation to the internet, ICT and COP. The findings are summarised in the following chapter.

3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

4 <https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf>

RAPID (MOBILE-LED) EXPANSION OF ICT IN RWANDA

Rwanda aims to position itself as the leading ICT hub in Africa, by 2024 (MITEC, 2018). To become ICT leaders in the region, significant investments have been made in ICT infrastructure, to improve access (see *Figure 1*).

- Over 1 year (2017–2018) the internet subscriptions have increased by approximately 25%
- The Government of Rwanda has made significant investments in ICT infrastructure, by installation of the 4000km fibre optic ‘backbone’, providing some homes in Kigali with access to wired internet
- The Government of Rwanda has made significant investments in ICT infrastructure, by deploying wireless 4G LTE technology throughout Rwanda
- 4G LTE, technology has been deployed throughout most (approx. 95%) Rwanda

Rwanda attributed rapid increases in internet service subscribers to the affordability and convenient use of smartphones, with competitively priced mobile-subscription internet bundles.

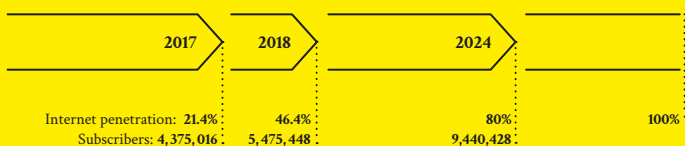
- Internet in Rwanda is almost exclusively accessed via mobile-broadband subscriptions
- Affordability schemes (e.g. mobile subscription internet bundles and public Wi-Fi hotspots) have been introduced to improve access for a broader demographic
- The Universal Access and Service Fund, established in 2004, funds multiple projects to increase access to basic ICT services for all Rwandans
- ‘Zero-rated’ services make popular content free and provide free data for regular internet users but these are not mitigated by local data protection laws
- WhatsApp and Facebook are popular subsidized services and among the most popular social media platforms, these services are also used as over-the-top services (i.e. an alternative means of communication)
- The Smart Kigali Program provides free Wi-Fi to public spaces, including commercial buildings, bus stations, hotels and public transport (over 485 buses have been equipped with public Wi-Fi)
- The Government of Rwanda recently announced plans to open a smartphone factory, Rwanda will be the first in Africa to manufacture smartphones for the African market, and will be able to offer payment plans and reduced prices to the Rwandan population
- By 2024, in line with the ICT Hub Strategic Plan, the Government of Rwanda aim to achieve an internet penetration rate of 80% and mobile subscription penetration rate of 98%.

By 2024, in line with the ICT Hub Strategic Plan, the Government of Rwanda aim to achieve an internet penetration rate of 80% and mobile subscription penetration rate of 98%.

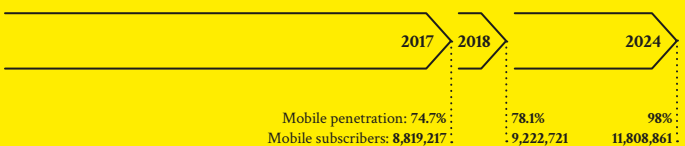
Figure 1

INTERNET AND MOBILE PENETRATION RATES IN RWANDA

Internet Penetration Rates In Rwanda



Mobile Penetration Rates In Rwanda



DIGITAL DIVIDES IN RWANDA

Rwanda is striving for all Rwandan citizens to access broadband and uptake the use of ICT. However, there are challenges in reaching this goal.

- Rwanda is ranked 9th out of 38 African nations in broadband affordability, but this may not translate into affordable prices for all users since 38.2% of the population are under the poverty line (2016/17 EICV5⁵)
- The populations' digital literacy rate is low at 8.4%, and many do not have the skills to use smart devices and utilise digital services
- Wired internet in the home is not possible for all, as many homes (73%) do not have access to electricity and only a small proportion, 3.2%, of households own a computer
- Rwanda is one of the few countries in Africa that provides 3G coverage to rural areas

Despite efforts to ensure that all Rwandan citizens are connected, there remain some persistent digital divides

The Rural Population

- The majority of the Rwandan population, 82.8%, reside in rural locations where ICT infrastructure is limited, and rates of penetration, uptake and literacy are lower
- The benefits of being online are less apparent to rural citizens
- The Universal Access and Service Fund supports projects to improve ICT access and use in rural areas (see *Figure 2*).

The Female Population

- Rwanda is recognised globally for its efforts to empower women, 52% of the population, and has implemented policies and legal reforms to promote and protect women's rights
- Gender gaps persist in literacy rates, including levels of tertiary, technical and vocational education. In these professions, and agriculture, women do disproportionate amounts of unpaid work, and anecdotal evidence suggests that where men and women work in similar occupations a wage gap persists
- Societal factors also prevent gender equality reforms from being enacted, e.g. the prevention of access to inheritance and exercising land ownership rights for women, or the 21% of women aged 20-24 who report that they were married before the age of 20, despite the legal minimum age for marriage for both men and women of 21
- Additionally, there is a high prevalence of gender-based violence (GBV), both in relationships (or former relationships) and more broadly by family members and beyond. GBV is highly correlated with economic disempowerment, which in turn impacts negatively on access and ownership of ICT devices as well as inhibiting the ability to freely use online services.
- Across Africa women are 13% less likely to own a mobile phone. In Rwanda, a recent survey reported an ownership gap of 21% (Female:37% vs. Male:58%)

Digital divides discussed below are recognised by the Government of Rwanda and both are discussed in the Ministry of ICT and Innovation's (MINICT) 2024 ICT Hub Strategy.

5 The Fifth Integrated Household Living Conditions Survey (EICV5) 2016/17 Rwanda Poverty Profile Report <http://www.statistics.gov.rw/publication/eicv-5-rwanda-poverty-profile-report-201617>

Figure 2

THE UNIVERSAL ACCESS AND SERVICE FUND PROJECTS

Projects active by end of 2009:

- › Rural Telephony Project
- › Low prices for Internet connectivity and Public access to Internet
- › One Laptop per Child Programme

Recent projects:

- › VSAT connectivity subsidy to all districts in remote and rural areas
- › Bandwidth connectivity of 30 Tele-centres managed by the Rwanda Development Board
- › Connectivity of secondary schools in remote and rural areas
- › Connectivity subsidy to 45 sites for the police in rural and remote areas
- › Connectivity of some private institutions and local businesses operating in rural and remote areas

Prospective projects:

- › Connectivity of all universities, public and private, using RWEDNET (Rwanda Education Network)
- › Connectivity of all technical secondary schools and all technical colleges
- › Connectivity of orphanages in two districts

Source: Ladcomm Corporation, 2014, p. 83

CHILDREN'S USE OF ICT

Academic literature on the Rwandan population in relation to ICT is scarce therefore, findings for the Rwandan population have been primarily collated from government and NGO reports.

- Approximately 60% of the Rwandan population is comprised of children and young adults (0-14 years = 40.98%, 15-24 = 19.45%)
- Only a small number (8%) of children aged 14-19 have access to the internet (5% sometimes, 2% often, and 1% regularly)
- Computer literacy amongst 15-19 year-olds is very low, at 5%, and digital literacy is likely to be lower in poorer households compared to wealthier households
- There is currently no information as to rates of mobile ownership or access for children (those aged under 18) in Rwanda

Rates of access to the internet and ICT technology are higher in schools than in the general population.

- Significant investments have been made to increase access to ICT in schools
- The Government of Rwanda have established a computer assembly plant and contributed approximately 25% of the total laptops provided to children under the One Laptop per Child programme
- There are plans to roll out 350 'smart classrooms' in both primary and secondary schools
- Plans to improve ICT education include the establishment of a new coding academy in the Nyabihu district to teach Rwandan students how to fight cybercrime, with further plans to construct 3 more coding academies in other provinces across the country

Despite significant investment in infrastructure for schools, schools lack sufficient resources, and continue to have shortages in classrooms, textbooks, labs, libraries and learning facilities.

- A significant number of schools still do not have internet access (in 2018: 52.9% of secondary schools and 30% of primary schools)
- Most students will not have access to ICT qualified teachers;
- Many schools suffer from a lack of electricity
- As of 2018, 63.9% of primary schools and 57.6% of secondary schools are owned by a denomination of the Christian church, rather than by Government (Government ownership is 25.3% for primary schools and 30.3% for secondary schools), which may impact on a COP curriculum
- Issues specifically affecting girls in schools, warranting further research and investigation, have been recognised in the 2015 Girls Education Strategic Plan
- There is a lack of formal policy in procedure relating to child protection and safeguarding

No available research was identified that specifically investigates Rwandan children's activities online.

- Research, not specific to children, states that local content is very popular in Rwanda, with local news sites⁶ and online public services⁷ being the most popular local sites

6 Examples cited: igihe.com and umuseke.rw

7 Example cited: irembo.rw

- Social media is also popular in Rwanda, with Facebook and WhatsApp⁸ being the most popular of the social media platforms
- The internet is also increasingly seen as important to enhancing business activities, work-related activities, seeking employment, education and to enhance social connections

ONLINE RISKS AND HARM, VULNERABILITIES AND PREVALENCE

- However, research on COP in the region (predominately from South Africa) does not currently use this terminology and generally refers to risk under the umbrella terms of cyberbullying, cyber aggression, and cyber victimisation
- Findings from these studies have focused on specific risks in these categories; and identified; experiencing or being exposed to: pornographic/sexual images; sexting; violent images; online fraud; cyber-bullying; racism & religious prejudice; threatening messages; teasing and name calling; hate speech; contact with strangers; and advertisements for/links to X-rated websites
- Studies vary wildly in determining prevalence rates of cyberbullying (umbrella term) suggesting victimisation rates of between approximately one third to over three quarters of children
- Victims of cyberbullying are found to experience a broad range of negative effects, including social, emotional, behavioural, cognitive, physical, mental, and academic achievement - victims of online bullying may also be bullied offline.

See Figure 3.

⁸ Even though these sites/apps (Facebook/WhatsApp) are also popular with UK children, it cannot be assumed that they are used in the same way. Further research would be required to determine how these sites/apps are used and how the environment appears to children.

Figure 3

TYPOLGY OF ONLINE RISKS

Research on COP in the global north is vast, and a typology of online risks has been developed. Risks are divided into 4 categories, namely content risks, contact risks, conduct risks and commercial risks.

- 1 Content risks: where children are exposed to harmful material (e.g. pornography, hate speech, violence);**
- 2 Contact risks: where children are involved in usually adult initiated online activity (e.g. grooming, stalking, sexual exploitation);**
- 3 Conduct risks: where children are victims or perpetrators in peer-to-peer exchanges (e.g. bullying, sexting, revenge porn); and**
- 4 Commercial risks: where children are exposed to inappropriate advertising, marketing schemes or hidden costs (e.g. targeted advertising, fraud, scams)**

Source: National Children's Bureau, Northern Ireland, 2014

CHILD ONLINE PROTECTION IN RWANDA

There were no identified studies on COP from Rwanda or based in Rwanda.

- The cyberbullying research centre⁹, which collates international research on COP, does not have any record of studies specifically centred in Rwanda and the academic databases searched for this review also failed to identify any specific material from the Rwandan context.
- There is acknowledgment of the need for child online protection, as demonstrated by the development of a COP policy by the Government of Rwanda, and its engagement with other international COP initiatives.
- This document notes that online harms may include child exploitation, child pornography, exposure to harmful and sexualised content, grooming, harassment, sexual abuse, cyber bullying, and sexting. Furthermore, virtual crimes can lead to offline sexual abuse, such as trafficking and sex tourism
- Additionally, emerging research globally places greater emphasis on everyday harms and opportunity costs, for example addictive use, sleeplessness, and over-exposure. Due to recent adoption and relatively low penetration, these issues are not yet on the agenda in the Rwandan context.

‘With the increase of information and data exchange on the network, protection of information, data, and people on the network is very critical.’

(RURA, 2018, p. 67)

- All available evidence asserts that Rwandan children’s access to ICT devices and the internet will increase rapidly over the next few years, which will correspond to both increased benefits of being online and increased risks.
- Rwandan children are arguably particularly vulnerable, due to the rapid increase in access, unawareness of all possible risks and no apparent safeguards in place.
- The COP policy will be introduced in the context of other initiatives e.g. ICT Hub Strategy 2024 and plans to improve cyber security and improve access to the rural and female population

The need to put measures in place is vital, to ensure that Rwandan children are safeguarded against all foreseeable risks (i.e. content risks, contact risks, conduct risks and commercial risks)

9 <https://cyberbullying.org/research/map#>

Respondent Interviews

The interviews with Rwandan stakeholders were undertaken to assess current response procedures and capability gaps, to inform policy development, strategies for implementation and to inform the communications strategy. This research was undertaken in collaboration with the University of Rwanda.

METHODOLOGY

- The qualitative research included 42 respondents (12 stakeholders and 30 HEI academics)
- Key local expert stakeholder interviews were conducted with 12 respondents, including educators, lawyers, advocates and government representatives
- The views of 30 academics from the University of Rwanda were gathered during a COP workshop
- The interviews followed the interview guide approach using open-ended questions each taking approximately one hour
- Interviewees were asked about their experience of COP issues in their respective fields, to describe any example cases, and were asked to consider how COP messages should be effectively disseminated in the community
- A thematic approach was employed to analyse the transcripts and to identify key findings
- The findings have been externally validated with reference to literature or sources from the region
- Findings are limited in scope given the scale and timing of the project but have been further validated by stakeholders who have engaged in other settings

KEY FINDINGS

- Respondents had limited knowledge of COP issues and online risks to children and all of the academic respondents stated 'no' when asked if they knew enough about COP
- Societal factors were cited as crucial to COP policy devising and implementing a successful COP policy;
 - Rwanda is a patriarchal society. There is a strong perception of what it means to be a 'good woman' which may hamper the adoption of some key concepts of child protection, specifically where they relate to girls

A good Rwandan woman is someone who is always patient, trying to protect their family, not claiming so much.

(Respondent A)

- Concern was expressed regarding the way in which westernized behaviour may impact negatively upon Rwandan cultural ideals. This concern has two parts – the responsibility of online services to consider local content including local languages and values, and how COP messages are imparted to local stakeholders, communities and children

Some African parents are trying now to be, I'm sorry I'm going to use this phrase, Westernized. They are no longer very private, in their romances ... there is a funny way of touching or behaving, and the children are watching. Then when you hear such and we see children exhibiting it, such as a 9-year-old boy trying to touch a girl in the class...

(Respondent B)

- When asked about knowledge of risks faced by children online, four key risks were identified; **exposure to pornography; unwanted teenage pregnancy; GBV in the online environment; and online security**. These offered insight into specific concerns as well as the capability and content gaps across the broader spectrum of COP issues

EXPOSURE TO PORNOGRAPHY

The risk that children are accessing pornography, both wilfully and inadvertently, was the primary concern of stakeholders (see *Figure 4*).

- Children accessing and being exposed to pornography is a concern that has been echoed in local media¹⁰
- It was suggested that primary school children are being exposed to pornography in the home whilst secondary school pupils are actively seeking out pornography while at school and on school devices (use of personal mobile phones is prohibited in most schools)
- The following comments were made
 - The affordability of internet packages and lack of restrictions on content allowed extended family members and house helpers¹¹ to expose children to pornography
 - This can result in children becoming victims of abuse, children attempting to act out inappropriate behaviours in schools (both sexual or violent) and/or experiencing sexual confusion
 - As well as accessing pornography, children are using school devices to watch other videos (e.g. YouTube), go on

10 For example: <https://www.newtimes.co.rw/section/read/219655> and <https://www.newtimes.co.rw/section/read/94913>.

11 Child Domestic Workers (CDWs) are “those under 18 working in household other than their own, doing domestic chores, caring for children, tending the garden, taking care of animals, running errands and helping their employers run small businesses, among other tasks. This includes children who ‘live in’ and those who live separately from their employers, as well as those who are paid for their work and those who are not paid and those who receive ‘in-kind’ benefits, such as food and shelter.” (Blagbrough, 2010, p. 82). See CLADHO’s publication (Domestic workers’ baseline survey focusing on child domestic workers and employers in Rwanda, 2015) for more information about CDWs in Rwanda.

Figure 4

CASE STUDY: CHILD EXPOSED TO PORNOGRAPHY

Facts as described by stakeholder:

- › A 7-year-old girl (grade 2) was found showing inappropriate pictures of a man to her friends in school. Picture was an advertisement for penis enlargement, with a man in his underwear.
- › The girl alleged another student, a boy, had tried to rape her in school.
- › The teacher reported that the same girl made multiple allegations against other students.
- › It transpired that a house helper, a boy, had originally shown her the pictures.
- › It also transpired that this house helper had been caught trying to get into the girl's bedroom to rape her. This was reported to the police.
- › The girl's home was also investigated. The teacher reported that the mother was watching inappropriate programmes and that the parents did not have a good marriage.
- › It was recommended that the girl be moved to a boarding school, as a result of her allegations.

Source: Interview with a Primary School Teacher in Kigali

- social media and illegally download materials
- Suggested interventions include more supervision in the home, becoming involved in extra-curricular clubs outside of the home, and installing security software on school devices (filtering software and age verification)
- The interviews highlighted the lack of formal child safeguarding policies and procedures in schools, as well as COP protections, and the need to introduce COP lessons into the school curriculum alongside sex education lessons
- Additionally, there was a desire for a greater understanding of child abuse issues (i.e. grooming behaviours), coordinated safeguarding procedures, victim support (i.e. how confused or traumatised child victims may act) and the skills or knowledge to respond to such incidences and recognise behaviours that may be indicative of abuse)

UNWANTED TEENAGE PREGNANCY

Concern regarding the rates of teenage (unwanted) pregnancy was an issue raised by multiple respondents (see *Figure 5*).

- Cases of unwanted pregnancies are increasing, and there are potential significant negative consequences to both the mother and child and wider communities

when we went in eastern province, they say that the perpetrators are mostly people who come for job in east, who are not permanent in their district. They come because there are some development activities, they come for short time, and they have money. For pregnancy issue. But when it comes to other rape, then it is neighbours, uncles, family members.

(Respondent A)

- It is acknowledged by respondents that unwanted pregnancy could be the result of abuse that is not reported by the victim
- Often what is actually being described is the rape of a child or the exploitation of children in the context of travel and tourism, yet these labels are not generally used and create some distance between the crime and the outcome for the child. Use of the correct terminology ensures that the described behaviours are understood as a crime and that the child is considered to be a victim of a crime
- The causes and interventions identified in relation to teenage pregnancy involve increasing sexual health awareness and providing contraception, but there remains a gap in awareness of child sexual abuse and a corresponding lack of enforcement of legal protections

Figure 5

RESEARCH FROM RWANDA ON UNWANTED TEENAGE PREGNANCY

Research projects by CLADHO and HAGURUKA have highlighted the causes and consequences of increased rates of unwanted teenage pregnancies:

Summary of CLADHO findings:

- › Nature of the issue: the rate of teenage (between 11-18 years) pregnancy is too high, and varies between 14.2-6.2% depending on district; in most cases (78.1%) the mother was 16 or above at the time of becoming pregnant; fathers were reported to be colleagues (49%), family friends (20%), strangers (17%), employers (6%), family members (4%), tutors (2%) and local leaders (1%).
- › A perceived cause is considered to be lack of knowledge (13% had knowledge of Adolescent Sexual Reproductive Health, 22% of Sexual GBV, 23% of human rights principles, and 31% of child's rights); that while use of contraceptives has increased from 27% to 54%, sexual and reproductive health rights programmes need to be expanded in schools. Another cause is considered to be coerced sex (87.7% of girls who had sex before the age of 18 reported that coerced sex contributed to adolescent pregnancy, 75% reported that sex, resulting in pregnancy, was coerced and 15% reported that sex was consensual). Poverty is a significant factor in both the cause and effect of teenage pregnancy.
- › There are various detrimental effects on both mother, baby, and the community. Teenage pregnancy has an adverse effect on the community, as many teenage mothers have to leave school, having an adverse impact on the individual and community in the long term. Many health problems can result from teenage pregnancy - babies to teenage mothers are at greater risk of being stillborn or dying in the first week or month of life, and babies born to teenage mothers are more likely to exhibit health problems. Most mothers are without financial support (98% do not receive support from fathers) and only 5% of babies were registered.
- › According to Rwanda Article 191 of the Penal code, child defilement (including cases of teenage pregnancy) is punishable by life imprisonment. The forced marriage of a minor, when age of consent to marry is 21, carries the same penalty. However, only 5% of cases were reported to the police and only 7.7% visited a hospital or health centre upon realising they were pregnant - most (59.2%) told a friend or family member. Furthermore, of the cases reported to the police, in only 8.6% was the perpetrator punished (<0.5% of the whole sample) and in most cases (58.3%) nothing was done.

- › Conclusions of this study were to improve education programmes and awareness, provide legal assistance to victims of GBV, institute zero-tolerance policies for teenage pregnancy and child marriage, and to improve access to medical care for teenage mothers.

Summary of HAGURUKA findings:

- › This research study was conducted in one province, so findings are less representative than the above study. Findings are focussed on cause of effect.
- › In this study, pregnancy was more likely to be a result of consensual sex than coercion (53% stated that sex was consensual and 32% stated that the sex was forced), therefore, teenage pregnancies are thought to result from an imbalance in sex negotiation, due to the fact that the male partners were almost always older; the mothers were not able to negotiate the conditions, resulting in non-consensual pregnancy. Lack of knowledge is considered to be a causal factor (one in five did not have knowledge of Sexual GBV).
- › As a result of pregnancy, teen mothers are rejected by their community and abandoned by the family and the male partner, only 73% of mothers had registered their child, and only 26% of male partners accepted to register their child. The identity of the father is often not disclosed, as both mother and father work to conceal his identity. The child is often left without medical insurance. 63% of teenage mothers were in school when they became pregnant, but only 5% were still in school by the time of the study.
- › Conclusions of this study were that teenagers need to have greater knowledge of GBV and their rights, greater knowledge of sexual health and family planning, and to improve access to survival means (e.g. schooling, integrated in society, access to work) for mother and child.

Sources: (CLADHO, 2016; HAGURUKA, 2018, pp. 39-41)

GBV IN THE ONLINE ENVIRONMENT

GBV is a broad term for crimes where there is a gender difference between the victim and perpetrator, and the following could be considered as issues underpinning exposure to pornography and unwanted pregnancy. GBV is typically thought of in terms of four categories; economical abuse, sexual abuse, psychological abuse and physical abuse.

- Whilst online abuse does exist, and more cases are beginning to emerge, current knowledge of how GBV manifests in the online environment and how such cases are investigated is sparse
- One respondent described a recent case of revenge pornography. It was not described using this terminology, but was described as sexual harassment and rape
- There has been media coverage of this type of abuse, with the aim of informing the public that it is a criminal offence¹²

yesterday, I received a case of a young lady, who come here to tell me that her boyfriend is harassing her. Because the boyfriend has a video, where during they were doing sex ... he's harassing her every time to say, if you don't come to see me for physical contact, I'll disseminate it through WhatsApp, then you will be ashamed.

(Respondent A)

- Strangers use social media, in particular Facebook, to target children (more frequently girls) and these interactions can result in sexual abuse or trafficking
- Those who are victims of abuse do not often report (as is the case in most countries), victims will only report abuse when it is their last resort, and victims of abuse are often ostracised by the families and their communities

we started receiving women, young women, coming at our office, saying that my parents want to kill me, because they don't want to see me anymore. Because they are saying, you have gone out of the country for money, for sexual activities, and how can you come back after 2 years and you don't even have money. I don't want to see you

(Respondent A)

- Awareness of abuse is very low, making it very unlikely that victims will report or know how to react to protect themselves
- A respondent working as a police officer commented that no reports of online child abuse or harassment had been received
- Even if victims were to report it is not clear how cases would be investigated, making it unlikely that perpetrators will be prosecuted

¹² <https://www.newtimes.co.rw/news/cyberbullying-sharing-nudes-be-criminalised>

- and that victims will receive adequate protection or support
- There is no specific COP legislation and so there is little technology or mechanisms in place to investigate online child abuse
- Suggested interventions included raising awareness in the community, specifically to young girls, with the message being that each individual is responsible for their security and should consider the consequences later in life of making videos with partners

ONLINE SECURITY

Security issues are apparent, e.g. accounts being hacked, fishing and spam emails, cold calling mobile numbers, theft of personal devices.

- Security online was acknowledged but seemed to be of much less concern than some of the other issues
- Concern for online security is also apparent in local media articles¹³
- The relationship between security (robust systems or high privacy settings) and COP was not raised and was perhaps not entirely clear to respondents
- The Government of Rwanda has been clear that with the rapid increase in use of ICT technologies, there is an increased risk of cybercrime
- Efforts to mitigate and minimise these potential threats include establishment of the Rwanda National Computer Security and Incident Response Team (Rw-CSIRT)¹⁴, and development of the upcoming National Cyber Security Policy¹⁵ and corresponding Implementation Plan (“National Cyber Security Strategic Plan”)¹⁶

FURTHER ISSUES

- Cyber bullying, and bullying in general, were not raised as a concern noting that there are educational schemes in place¹⁷ that safeguard against bullying, by encouraging children not to focus on each other’s differences

bullying? No that is not a problem, actually we try to deter it ... we have to stop it. Because when they come, the new ones, we tell them that there is no bullying here, no teasing, based on our past history. Because some abuse it.

(Respondent D)

¹³ See <https://www.newtimes.co.rw/section/read/222755>, <https://www.newtimes.co.rw/news/cyberbullying-sharing-nudes-be-criminalised> and <https://www.newtimes.co.rw/section/advertorial/1007>

¹⁴ <http://rw-csirt.rw/eng/>

¹⁵ <http://minict.gov.rw/policies-publications/policies-and-regulations/policies/upcoming-policies/>

¹⁶ http://minict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/NCSP_Implementation_Plan.pdf

¹⁷ <https://www.aegitrust.org/what-we-do/activities/students-youth/rwanda-youth-programmes/>

- Despite internet use being low there are already concerns about its impact on daily life with a strong feeling that the internet should be reserved for productive activities only, such as homework, or that children should spend less time online and more time outside
- There was little or no discussion about compulsion or addiction
- The call for local values and local content should be noted

COMMUNITY AWARENESS AND PUBLIC MESSAGING

Many stakeholders would like to see increased COP awareness through simple messaging.

- Previous successful messaging campaigns discussed included initiatives to reduce littering, awareness of landmines in 1994, and a recent campaign to raise awareness about domestic violence and women's rights
- There are two key components of developing and running a successful communications strategy in Rwanda
- Simplicity in terms of messaging which should be largely image-based particularly given the high illiteracy rate
- An awareness of the social leadership structure. This leadership structure has also been found in publications¹⁸
- Forums are held in sector meetings. In these meetings 'Grass roots leaders' come together to meet and discuss important issues impacting upon society
- There are forums for local leaders, parents, and children. These forums and the National Youth Council should be approached about COP issues¹⁹
- In such meetings the use of images or use of role playing can be used to prompt a discussion about the issues in question, those in attendance evaluate the situation presented, anticipate the potential effects and brainstorm interventions
- Issues discussed at sector level and are then taken by leaders back to their communities to be shared
- Information dissemination channels are effective in Rwanda; to effectively raise awareness of any issue information must be shared in this way
- Information is also shared during Umuganda - when all able persons aged 18-65 carry out community work (e.g. cleaning and repair in the community) and discuss issues affecting the community²⁰ - on the last Saturday of every month.
- Sharing information via media outlets, T.V. and radio, and use of brochures and banners would be effective but given the low literacy levels are not the most effective way to reach all of the community

See Figure 6.

18 https://www.un.org/womenwatch/ianwge/taskforces/vaw/VAW_COUNTRY_ASSESSMENT-Rwanda-1.pdf

19 <https://nyc.gov.rw/index.php?id=3>

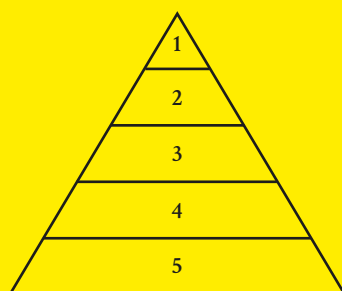
20 <http://www.rgb.rw/index.php?id=37>

Figure 6

LEADERSHIP STRUCTURE IN RWANDA

| | | |
|---------|--|---------|
| Level 1 | PROVINCES Led by Kigali, Governors, and Mayor | × 4 |
| Level 2 | DISTRICTS Led by District Mayors | × 30 |
| Level 3 | SECTORS Led by Executives | × 416 |
| Level 4 | CELLS Led by Coordinators | × 2150 |
| Level 5 | VILLAGES | × 14953 |

Source: (UNFPA, 2008, p. 6)



RAISING AWARENESS IN SCHOOLS

Respondents were keen to incorporate lessons on COP in primary and secondary education curricula, alongside improving digital literacy for students and for parents.

- There was deemed to be a role for external organisations, such as Plan International who have previously delivered awareness, but there was a great appetite for teacher training and curriculum development in COP
- Educating parents on COP issues to prevent harms originating from internet use at home could be done by schools and trained teachers
- COP sessions must be taught in the context of key issues on healthy and appropriate sexual relationships, particularly in the context of wider concerns around the high teenage pregnancy rate, sexual health and GBV.
- COP awareness in schools should incorporate digital literacy and encourage children to use the internet in positive ways, i.e. ensuring the positive use of technology and creating a scaffolding for acquiring digital skills
- Alongside raising awareness in schools, software should automatically be installed on computers in schools to prevent students from accessing or being exposed to harmful content
- All schools should also develop standardised COP school policies and procedures

CONCLUSION

There is an urgent need for greater understanding and awareness of COP issues across a broad set of policy areas and audiences. There must be an increasing emphasis on multidisciplinary working, COP and safeguarding training and support for all frontline workers. Technical controls are few and far between in both homes and schools, and as devices become more prevalent, consideration should be given to supplying them with up-to-date safety features. In particular we note the anxiety about Western influences and gender imbalance form the backdrop to COP concerns in Rwanda.

Findings from the Respondent Interviews and Background Information were used to shape the development of the Child Online Protection Policy Chapter, the Five-Year Implementation Plan and the Communications Strategy. A gap in the enforcement capabilities was also identified, which resulted in a workshop in Scotland for Rwandan leaders (Appendix D) and a bespoke COP framework was developed at the request of the respondents (Appendix A)

These findings have implications beyond the context of this project, highlighting key social issues that will impact upon the successful implementation and effectiveness of child online protection policy and practice.

Child Online
Protection
Policy Document

The document below is the document submitted to Minister of ICT and Innovation on 20th February 2019. After a period of interdepartmental and further stakeholder consultation a small number of changes were made. The final document "Rwanda Child Online Protection Policy" can be found here²¹. It was formally adopted on June 25th 2019. We applaud the Government of Rwanda for adopting the COP Policy. The changes are summarised below.

- The 10 values outlined (5.1) were replaced by a commitment to uphold Rwandan values more generally. Rwandan values are articulated, published and used widely as a tool of policy and civil life.
- Public Awareness was integrated with education as a single section. Whilst much of the text remains the same, including commitments to teacher training, and broad digital literacy programmes in both education and for the general public, the training for all relevant professions (i.e. in social work/enforcement etc.) and regular updating of COP training were removed.
- The proposed Steering Committee was renamed an Advisory Committee and the proposed COP Stakeholder Group renamed COP champions (which builds on existing structures). The role of civil society organisations/ISP/industry in the COP champions group has become more advisory.
- The requirement for industry standards to be mandatory and overseen by MINICT was removed.
- Added internet surveillance and CSAM database to the technical solutions section (5.4.4)
- Downgraded the commitment to funding R&D and the creation of Rwanda as a centre of COP excellence, whilst retaining a commitment to do the research itself.

21 https://minict.gov.rw/fileadmin/Documents/Policies2019/COP_Policy_Updated.pdf

1. INTRODUCTION

The Internet and associated digital technologies provide opportunities for social and economic transformations that benefit all sections of Rwanda's society, including children. However, the use of digital technologies comes with some known risks and harms for children. The Rwanda Child Online Protection Policy ("the COP Policy") is designed to mitigate against those risks and harms, and to deliver a framework that meets children's needs and fulfils their rights, while enabling them to safely and confidently navigate the digital environment.

Rwanda considers children's rights to be a pillar of public policy, as evidenced in its institutions, policies and laws.²² Realising children's rights in a digital world involves a broad spectrum of stakeholders, each of whom must act in the best interests of the child.²³ All stakeholders, including government and government agencies; information and communications technology companies (including hardware and infrastructure companies); communities and civil society organisations; parents, teachers and children themselves must accept and exercise a shared responsibility in the implementation of this policy, in line with their respective roles and resources.²⁴ In framing the COP Policy, it has been important to consider the asymmetry of knowledge and access to expertise between those who create technology and those who use it. Comprehensive child online protection is dependent upon stakeholders working in partnership; nationally and internationally.

The COP Policy includes the establishment of a governance system which will act as a central point for the direction of all policy areas. The Governance system shall coordinate existing domestic regulatory and legislative frameworks to harmonise legislation with global best practice; strengthen the understanding and capacity of law enforcement; further the provision of education, information and training for all stakeholders, including parents and children; establish a high level of data protection, with specific provisions for children; create world-class reporting and takedown mechanisms; and promote positive uses of digital technologies by children. These efforts will build on Rwanda's existing strides towards protecting children online and establish the country as a regional leader in COP research and innovation.²⁵

The COP Policy reflects the fact that the digital environment is a significant tool for children's education, creativity, self-expression and economic empowerment, and that children's access to the digital environment is both necessary and desirable. It represents the Government of Rwanda's full commitment to the safety and wellbeing of children, the nation's greatest and most precious asset.

22 Under Article 1 of the UN Convention on the Rights of the Child, children are generally recognized as persons under the age of 18; in Rwandan law (N°54/2011 OF 14/12/2011), a child is any person under the age of eighteen (18) years old.

23 Convention on the Rights of the Child, Article 3.

24 In determining responsibilities, it is important to consider stakeholders' knowledge, resources and capacity, and in particular the imbalance in power between those who create technology and those who use it.

25 Among other things, Rwanda has a 24/7 Cyber-Security Incident Response Team, a Cyber Forensic and Investigation Laboratory Centre, and Hotlines through the Police and the National Children's Commission.

26 Convention on the Rights of the Child (1989), http://www.unesco.org/education/pdf/CHILD_E.PDF

27 World Summit on the Information Society, Outcome Documents (2005) <http://www.itu.int/net/wsis/outcome/booklet.pdf>

28 World Summit on the Information Society, Tunis Commitment (2005) <https://www.itu.int/net/wsis/docs2/pc3/working/dt12rev5.pdf>

2. INTERNATIONAL AND REGIONAL CONTEXT

The digital environment is transnational; therefore, it is important to consider international agreements, standards and guidance relevant to COP. The United Nations Convention on the Rights of the Child (CRC) sets the gold standard for children's rights and applies online just as it does offline. The CRC enshrines children's rights to protection from violence and exploitation, privacy, participation, freedom of expression, and association, among others²⁶.

The World Summit on the Information Society's (WSIS) Outcomes Document²⁷ and Tunis Commitment²⁸ recognise both the role of ICTs in enhancing children's development and the need to protect children from abuse and uphold their rights in a digital world. Similarly, the UN Sustainable

Development Goals (SDGs) provide a roadmap for international cooperation and development, and set targets related to education, industry, innovation and infrastructure that will shape children's access to and experiences in the digital environment. The SDGs also call for an end to all forms of abuse, exploitation and violence against children.²⁹

As part of the Global Cybersecurity Agenda (GCA)³⁰ the International Telecommunication Union (ITU) has developed COP Guidelines for policy makers; parents, teachers and educators; children; and – with UNICEF – industry.³¹ These Guidelines aim to establish the foundations for a safe and secure digital environment. The WeProtect Global Alliance, led by the UK Government, also produced a Model National Response to prevent and tackle online sexual exploitation and abuse.³²

The African Charter on the Rights and Welfare of the Child (ACRWC)³³ and the African Youth Charter (AYC)³⁴ set out the rights and duties of children.³⁵ Much like the CRC, the ACRWC and AYC recognise children's protection and participation rights. The African Union's 2040 Agenda for Children aspires for all African children to be protected against violence, exploitation, neglect and abuse, to be given opportunities to share their views in society, and to have access to quality education that integrates digital technology.³⁶

The COP policy seeks to build on and manifest all of these standards in the Rwandan context.

3. CHILD ONLINE PROTECTION IN RWANDA

Rwanda has a young population. Children, defined as persons under the age of eighteen³⁷, constitute nearly half the population³⁸. Rwanda is actively seeking to improve access to the Internet and digital technology, to embrace the use of smart technology on a city scale, and to transition government, banking and commercial operations and services to digital platforms. At the time of policy development, 52.8% of the Rwandan population are online, an over 25% increase over the previous years³⁹. The COP Policy anticipates a time in which all children in Rwanda are online and embodies the need to ensure that they are empowered, protected and their rights promoted in the digital environment.

Rwanda has already developed a favourable policy environment for digital technology, children's rights and cyber security, and has taken specific steps to meet some of the challenges. However, both the complexity of the digital environment, its changing nature and defining a child's place within this environment require further action to be taken.

Existing initiatives include: National Cyber Security Incident Response Team, Digital Forensic Laboratory, Police Toll Free, laws to facilitate prosecution for cybercrimes, including the advertising of child sexual abuse material (CSAM)⁴⁰, Campaigns and Awareness Programmes, Community Policing Programme, International Cooperation Initiatives (e.g., with Interpol and other law enforcement agencies; signatory to coordinated global action to forge partnerships with industry to tackle online sexual abuse).

4. POLICY RATIONALE

The Internet and digital technologies provide children with an unprecedented range of opportunities to play, learn, innovate and be creative; to communicate and express themselves; to collaborate and engage in society; and to develop

- 29 For more information about the Sustainable Development Goals, visit: <https://www.un.org/sustainabledevelopment/sustainable-development-goals/>.
- 30 ITU Global Cybersecurity Agenda, High-Level Experts Group, Report of The Chairman, <https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf>
- 31 For the full set of COP Guidelines, visit <https://www.itu.int/en/cop/Pages/guidelines.aspx>.
- 32 WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse: A Model National Response (2015), available at <https://www.weprotect.org/the-model-national-response/>.
- 33 African Charter on the Rights and Welfare of the Child (1990), http://www.achpr.org/files/instruments/child/achpr_instr_charterchild_eng.pdf
- 34 African Youth Charter (2006), https://au.int/sites/default/files/treaties/7789-treaty-0033_-_african_youth_charter_e.pdf. The AYC applies to persons aged between 15 and 35.
- 35 Rwanda ratified the ACRWC in 2001 and the AYC in 2007.
- 36 Africa's Agenda for Children 2040, African Committee on the Rights and Welfare of the Child, https://au.int/sites/default/files/newsevents/agendas/africas_agenda_for_children-english.pdf. See also African Union Assembly adopts 2040 Agenda for Children, International Justice Resource Center (Aug. 14, 2017), https://au.int/sites/default/files/newsevents/agendas/africas_agenda_for_children-english.pdf.
- 37 Law N°54/2011 OF 14/12/2011.
- 38 According to the latest 2015 UN figures, 52% of the population is under 20 and 42% is under 15. The projection for 2020 is for 49.5% to be under 20. See <https://population.un.org/wpp/DataQuery/>
See also census data for 2012: <http://rwanda.opendataforafrica.org/mlhmqxf/rwanda-census>
<http://rwanda.opendataforafrica.org/twedwyc/age-structure-of-population>
- 39 Rwanda Utilities and Regulatory Authority (RURA), Annual Report 2017-2018 http://www.rura.rw/fileadmin/Documents/docs/report/RURA_ANNUAL_REPORT_2017-2018.pdf
- 40 See, e.g., Official Gazette no. 14 of June 2012, Article 30.

21st century digital skills.⁴¹ Children should be encouraged to develop creative and digital skills, and be empowered to exercise their full range of rights online, in a safe and secure way.

The COP Policy sets out a comprehensive set of policy areas and measures designed to support children online, in an environment where all stakeholders play their part.

The digital environment rests on fast-changing technology that since its introduction, has become extremely powerful in dictating the behaviour of children and young people. Being online gives children access to information, facilitates human contact, and enhances commercial exposure. It is for this reason that Rwanda seeks to establish its requirements of all stakeholders regarding the protection and privileges of child users.

4.1 RISKS AND HARMS

Evidence shows that children face many of the same online risks regardless of geographical location, but there are some specific concerns in nations where the expansion of digital access has happened rapidly and recently. Some harms may only emerge when digital technology has been widely adopted and extensively used. Therefore, it is necessary to consider evidence of harms from other contexts, the specific issues and relative importance of risks as they manifest in the Rwandan context, and to anticipate risks that may emerge in the future.

Risks do not inevitably result in harm, and it is vital to understand the factors that give rise to the probability of harm to children. Risks fall into four broad categories (content, contact, conduct, contract)⁴²:

Content risks include: indecent images of children, adult pornography, violent, discriminatory or hateful content, fake news or false narratives, content that promotes risky or unhealthy behaviours.

Contact risks include: child trafficking, discriminatory abuse and hate speech, grooming and exploitation, harassment, radicalisation, blackmail, unwanted sexual advances, sharing the real time location of a child.

Conduct risks include: bullying, sexting, revenge porn, threats and intimidation, reputational damage, impersonation, social humiliation, compulsive use, cybercrime, gambling.

Contract risks (sometimes called commercial risks) include: data collection for targeted advertising, marketing schemes, fraud, scams, misuse and misappropriation of intellectual property, unfair terms and conditions, and weighted search rankings. This includes commercial drivers which create norms that children are developmentally not able to manage or absorb without harm (e.g., profiling vulnerable users, inaccurate or discriminatory socio-economic profiling, automated/semi-automated decision-making and data set training, loss of control of digital legacy/footprint, surveillance by public and commercial institutions).

Harms

The experience of harm changes from child to child on the basis of factors including but not limited to gender, age, family circumstances, socio economic status, and experiences and availability of digital technology. Child online protection strategies must be developed in advance to mitigate risks and address harms, and to always consider how products and services may negatively impact the end user, if that user is a child.

41 See OECD, *The Future of Education and Skills: Education 2030, The Future We Want*, available at [https://www.oecd.org/education/2030/E2030%20Position%20Paper%20\(05.04.2018\).pdf](https://www.oecd.org/education/2030/E2030%20Position%20Paper%20(05.04.2018).pdf).

42 <http://www.safeguardingni.org/sites/default/files/sites/default/files/imce/E-safety%20report%20exec%20summary%2000114.pdf>

5. NATIONAL CHILD ONLINE PROTECTION POLICY

5.1 VALUES

To respect one another = KUBAHANA

To be gracious and hospitable = KUGIRA UBWUZU N'URUGWIRO

To respect family = KUBAHA UMURYANGO

To be a patriot = GUKUNDA IGIHUGU

To be selfless and kind = KUGIRA UBWITANGE

To be heroic and willing to act = KUGIRA ISHYAKA N'UBUTWARI

To act against discrimination = KWIRINDA IVANGURA

To protect public resources = GUCUNGA NEZA IBYA RUBANDA

To care for the security and safety of others = KUBUNGABUNGA UMUTEKANO

To uphold the values of Rwanda = KIRAZIRA KUGAMBANIRA IGIHUGU

5.2 VISION

All Rwandan children are empowered to access the digital environment creatively, knowledgeably and safely.

5.3 STRATEGIC OBJECTIVES

- Establish a governance framework to drive and guide COP delivery and enforcement
- Educate all stakeholders in COP principles, including safety, security, data protection and children's rights
- Adopt technical mechanisms that safeguard children and support productive and autonomous use of digital technologies by children
- Position Rwanda as a centre for excellence of COP research, evaluation and innovation
- Promote national, regional and international cooperation on COP
- Build an iterative process in which COP Policy is continuously reviewed and improved

See the Resources Directory (pp. 71)
for supporting materials for section 5.4.

5.4 POLICY AREAS FOR CHILD ONLINE PROTECTION

5.4.1 POLICY AREA: COP INSTITUTIONAL CAPACITY

Objective:

To establish a National COP Steering Committee and to establish a Stakeholder Group of experts to cover all areas of the COP Policy, coordinated by the Ministry of ICT and Innovation (MINICT).

Measures:

- A Publish a definitions and language manual: The Ministry of ICT and Innovation will publish a full list of definitions and language that reflect definitions used in international agreements.
- B Establish a National COP Steering Committee: The National COP Steering Committee will be responsible for policy implementation and development, and will serve as a focal point for national, regional and international cooperation. The Committee will address a broad set of competencies that cover all policy areas, and will supervise implementation and uphold standards.
- C Create a COP Stakeholder Group: A COP Stakeholder Group will be made up of both full-time COP professionals and designated focal persons (“COP leads”) to advise the National COP Steering Group and serve as COP advocates in their own institutions and organisations. Specifically, The National Children Commission (NCC) will establish and designate a fully resourced desk department with experts in COP. Similarly, key institutions including Ministry of Justice, Rwanda National Policy, Rwanda Investigation Bureau and National Public Prosecution Authority shall consider designating positions with full-time experts to handle COP matters. Other stakeholders, including business enterprises and civil society organisations, will be asked to designate two or more COP Leads to participate in the Stakeholder Group.
- D Define roles and responsibilities of stakeholders: There will be a co-regulatory framework that defines the roles and responsibilities of all organisations developing and managing digital infrastructure, networks and services. In particular, there will be guidelines for hardware donated to schools or children to ensure that devices are equipped with appropriate safety filters and software and that COP training is provided to those introducing and overseeing the use of such equipment, to ensure safety features provided are operational and can be modified appropriately with age and capacity.
- E Define performance indicators and evaluation: Each aspect of the implementation plan will have a corresponding expert coordinator with the authority and resources to successfully complete the task envisioned. Key Performance Indicators (KPIs), evaluation mechanisms and clear reporting structures will be introduced. As the digital environment evolves rapidly, KPIs will require constant review.

5.4.2 POLICY AREA: LEGAL AND REGULATORY FRAMEWORKS

Objective:

To strengthen and re-align the domestic legal and regulatory regimes related to COP, and to strengthen the capacity and capability of law enforcement agencies.

Measures:

- A **Strengthen the capacity of law enforcement agencies.** From first responders to judges, all actors in the law enforcement chain must be

aware of COP. They will be offered training, including on how COP relates to their particular role, how to understand offending behaviour, and how to provide access to victim support. Shortcomings in enforcement and the judiciary will be identified, and measures will be put in place to increase awareness, reporting and successful prosecution. Cross-sector coordination and collaboration between industry and law enforcement will be encouraged.

- B Strengthen and enforce laws that prohibit COP-related offences.** Criminal laws and procedures facilitate the investigation and prosecution of online offences that violate children's right to protection, and will be strengthened and amended in line with international standards and best practices. This will include enhancing sanctions and sentencing frameworks where necessary.
- C Introduce data protection regulations, ensuring that children's data is protected appropriately, collected only where necessary with high levels of security and care.** Such general regulations should include children's data given special category status, requiring higher levels of protection and other safeguards, and the introduction of parental consent for the online collection and processing of younger children's data.
- D Strengthen criminal investigation, prosecution and sentencing for online child sexual abuse⁴³:** Criminal justice agencies with responsibilities for COP-related offences will be trained in COP issues, particularly in respect of online child sexual abuse, with the aim of driving greater prevention, successful prosecution and appropriate sentencing. The capabilities of the Rwanda Computer Emergency and Security Incident Response Team (Rw-CSIRT) and the Police Cybercrime and Investigation Centre shall be reviewed and strengthened to detect, prevent and respond to cyber security threats, specifically those related to COP.
- E Identify and ratify COP-related international treaties & protocols:** Building a sustainable eco-system of COP requires a multi-stakeholder approach and participation in a global movement. Rwanda will identify and ratify relevant international and regional protocols and treaties.

5.4.3 POLICY AREA: COP RESPONSE SYSTEM

Objective:

To establish a coordinated multi-stakeholder framework to tackle online child abuse.

Measures:

- A Establish methods of notice and takedown:** Government institutions will work with industry to establish and monitor effective protocols for the notice and takedown of illegal child abuse material (CAM), and establish protocols to ensure, and legislation to permit, local ISPs to block access to hosts that fail to take down notified content.
- B Establish process of offender risk management:** An effective multi-stakeholder offender management process will be established, drawing upon international standards of good practice. Law enforcement and other criminal justice practitioners will be trained to recognise and investigate offending behaviours. Offender risk management is an essential component of COP, as individuals or groups of offenders can reach large numbers of child victims online.
- C Provide support for child victims:** Organisations training practitioners in the mental health, psychology and social work fields who work with

⁴³ Child sexual abuse (CSA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline.

vulnerable children must be required to have a basic understanding of COP issues. A key aim in prevention of online harm will be to consider the needs of vulnerable children and how to best support them. The capabilities of all One Stop Centres will be strengthened to follow safeguarding and child protection procedures, provide support for victims, and escalate reports of online crimes to the relevant authorities. To be effective, relevant practitioners must be provided with COP training, training on safeguarding and child protection policies, training on child counselling (to help children process trauma and prevent further victimisation), and training on family counselling (to prevent child victims from being ostracised by family members and being further victimised).

5.4.4 POLICY AREA: TECHNICAL CONTROLS

Objective:

To promote safety-by-design, corporate responsibility and cultural awareness of COP.

Measures:

- A** Introduce corporate responsibility standards: Industry has a responsibility to ensure that children are afforded protection online. In line with Rwandan values (see section 5.1), businesses will be required to show what procedures and special considerations they have undertaken to ensure child safety and respect for children's rights as they extend their online services into Rwanda. The code will be created by the ministry, overseen by the Steering Committee, and these standards will be mandatory.
- B** Implement safety, rights, ethics by design: Standards and codes of practice will be developed to require product designers, manufactures and service providers to uphold Rwandan values (see section 5.1) and contribute to children's online safety and security. Among other things, standards and codes of practice will aim to prevent children from seeing harmful or inappropriate content; to protect children's online privacy on the system or device-level; and to address concerns raised by the Internet of Things, connected toys and services with a streaming function
- C** Application of age-rating classification: Consistent age-rating and classification of commercial content offers a transparent and effective approach to manage content and services accessed by children and may be required for relevant goods and services.
- D** Introduce flagging systems: Mechanisms to identify and report upsetting or unsuitable content will be required of the service providers, and transparent and robust monitoring systems must be in place for all online services. A free public hotline will be available for reporting and accessing specialist support and advice and provision of takedown mechanisms.
- E** Ensure protection of children from commercial pressures: Efforts to protect children from commercial pressures will include: providing content filters, promoting safety-by-design, and raising awareness of the context in which children grow up. Products and services that are offered in line with Rwandan values (see section 5.1) may be certified, and action may be taken against purveyors of products and services that violate these values.

5.4.5 POLICY AREA: COP EDUCATION

Objective:

To positively promote use of digital technology as a source of entertainment, information and educational content for children in a safe environment.

Measures:

- A Designate Child Protection Leads: Each school is to designate a Child Protection Lead. Each lead is to be provided with training on child protection procedures and to be provided with COP specific training. Leads will be responsible for enacting and enforcing child protection policies (including safeguarding procedures) in schools, be the point of contact for concerns relating to child protection and COP, and pass on reported harms to the relevant authorities. Leads should also facilitate intervention plans, to protect children against further harms.
- B Promote edutainment: Promote content, including peer-to-peer programs, designed to educate through entertainment that helps children develop digital skills and empowers children to build respectful communities.
- C Promote educational content: As digital adoption becomes widespread, pupils and teachers will be taught the necessary skills for interacting with digital systems to fully benefit from curriculum content, both in local languages and international languages.
- D Promote digital literacy: A programme of digital literacy will be introduced across the school curriculum. The programme will emphasise and encourage the positive, autonomous and creative use of digital technologies by children; clearly define the risks, benefits, and social outcomes of using technology; and will aim to ensure that protective and preventative measures are broadly disseminated, understood and applied.
- E Introduce formal COP procedures in schools: COP training must form a mandatory part of teaching degrees, at primary and secondary school level. All teachers must complete mandatory training on COP, be aware of school policy in relation to COP, and deliver COP lessons to students. All Schools must appoint a COP lead to champion COP standards and enforce school policy on COP.
- F Build tertiary education schemes: COP sessions must form a mandatory part of teaching, social work, health work, psychology and other relevant degree programmes in public and private universities. There is a need for regular review of the effectiveness of these degree lessons, in light of advances in COP training and emerging issues.
- G Encourage professional development: Continuing education programmes on COP and child safeguarding for professionals working in relevant fields will be established, regularly reviewed and updated to keep pace with emerging technologies and address new barriers and concerns as they become apparent.

5.4.6 POLICY AREA: PUBLIC AWARENESS

Objective:

To raise awareness of all COP issues, in order to prevent likely harms and promote positive Internet use. This information will be disseminated widely, with specific programmes for different audiences.

Measures:

- A Generate public awareness programme: Awareness-raising strategies will produce materials that make clear the principles of COP and actions that can be taken to mitigate harms, report offences and seek redress. This information will be provided in simpler terms on the Ministry of ICT and Innovation's webpage. Targeted messages and materials will consider the specific needs of parents and children, with particular attention given to the youngest and most vulnerable children, including those with learning disabilities. Peer-to-peer education is a valuable strategy for children of all ages to get to know their rights and responsibilities online. This programme of public messaging can help children and adults to understand the issues and make wise choices about their online interactions, but is not a replacement for formal education, professional training, safety-by-design or corporate responsibility.
- B Provide informal education: Online safety education will start in early childhood and develop according to children's changing needs as they grow; specific materials will be produced to guide children of preschool age, caregivers and teenagers. Information will promote positive use of digital technology and consider the needs of all Rwandan children, regardless of gender, age, income or background. Information provided by third parties will be expected to include the values articulated in the COP Policy and aim to help children of all ages to get to know their rights and responsibilities online. Community groups, youth clubs, families, churches and digital platforms will all be instrumental in driving effective COP education.

5.4.7 POLICY AREA: COP RESEARCH & DEVELOPMENT

Objective:

To establish a COP research and innovation hub for the region.

Measures:

- A Establish COP research frameworks: Rwanda will establish a central research fund to develop a research programme with clearly identified terms of reference and objectives that remain current, in order to enable ongoing research in COP across a broad range of relevant issues.
- B Continued innovation: Research evidence will inform the development of products and services that incorporate safety-by-design; enable the evaluation of COP practice; and provide an understanding of children's online experiences in the Rwandan context.
- C Institute centre of excellence in research and development in COP: Rwanda will position itself as a regional hub that exports tools, services and skills about COP through national, regional and international engagement.

5.4.8 POLICY AREA: COP GLOBAL COOPERATION

Objective:

To collaborate with national, regional and global organisations and players to share best practice.

Measures:

A) Establish formal relationship frameworks (MoU) with regional and global COP communities: Strengthening international cooperation to enhance COP across the globe is critical to guarantee global security. Rwanda will formalise collaborations for joint PPP investments in areas related to cyber-security, COP capacity building, innovation, law enforcement, the justice system and education, among others.

Child Online
Protection
Five-Year
Implementation
Plan

In forming the COP Policy, our expert panel (Further Resources – Contributors) made it clear that whilst a high-level policy document was required, that without some ‘steps’ to implementation – the policy alone did not provide enough guidance. This view was mirrored by Rwandan stakeholders, and as the policy developed there was an increasing interest in understanding how policy might be implemented. As a result, we expanded our work to include a high-level five-year implementation plan. The plan directly follows the framing and numbering of the policy document. It also mirrors the thinking behind the WePROTECT Global Alliance Model National guidance to prevent and tackle child sexual exploitation and abuse (CSEA)⁴⁴ which puts a premium on leadership, multi-stakeholder responsibility, and joined up response. In collating this document we were privileged to have the input of our expert group, who provided many best practice and practical examples of COP implementation – these can be found in Appendices D & E.

The implementation plan suggests a gradual approach whereby each policy area and aspect of COP has its own journey, but each aspect can be seen in relation to each other. It is perfectly possible that one policy area may be implemented faster than proposed, whilst another may suffer set-backs. However, whilst any single path can be pursued without impacting on the other, it remains a fact that COP is a genuinely interconnected and networked policy area. It is unlikely that effective COP will be achieved without all aspects being fully realised.

44 <https://www.weprotect.org/the-model-national-response>

Five-Year Plan Enablers

In forming this policy, it was necessary to create an implementation plan. Each area has a waterfall effect in that the requirements for Year 1 must be completed before those for Year 2. It is also the case that certain enablers, universal to enacting effective policy, were identified. They are:

Leadership

Cross-discipline working

Clear reporting structures

Hearing the voice of children

Community buy in

Clear goals

Regular evaluation and review

| | 5.4.1 | | | | 5.4.2 | | | | | | | 5.4.3 | | | 5.4.4 | | | 5.4.5 | | | | 5.4.6 | | 5.4.7 | | | 5.4.8 | Key |
|------------|---|--|---|--|--|---|--|--|---|---|--|---|--|--|--|---|---|---|---|---|--|--|--|--|--|---|--|-----|
| | INSTITUTIONAL CAPACITY | | | | LEGAL AND REGULATORY | | | | | | | RESPONSE SYSTEMS | | | TECHNICAL CONTROLS | | | EDUCATION | | | | PUBLIC AWARENESS | | RESEARCH AND DEVELOPMENT | | | GLOBAL COOPERATION | |
| | Measures | National COP Steering Committee | COP stakeholder group | KPIs & Evaluation | Legal and regulatory Capacity Building | Strengthen Laws and Legislation | Strengthen Data Protection Regulations | Criminal Investigation, Prosecution and Sentencing | Ratifying Existing Protocols | Removal of Material | Offender Management | Victim Support | Corporate Responsibility | Protection from Commercial Pressure | Safety and Security Features | COP in Schools | Positive Use of Internet | COP for Professionals (Tertiary Education) | Professional Development | Public | Targeting Parents & Young Children | COP Research | Innovation | Centre of excellence | Regional & Global Partners | | | |
| | 5.4.1 A&B | 5.4.1 C&D | 5.4.1E | 5.4.2 A | 5.4.2 B | 5.4.2 C | 5.4.2 D | 5.4.2 E | 5.4.3 A | 5.4.3 B | 5.4.3 C | 5.4.4 A&B | 5.4.4 E | 5.4.4 C&D | 5.4.5 D | 5.4.5 A-C | 5.4.5 E | 5.4.5 F | 5.4.6 A | 5.4.6 B | 5.4.7 A | 5.4.7 B | 5.4.7 C | 5.4.8 A | | | | |
| 2019 | Obtain explicit commitments from government and public sector to put COP policy at heart of operations. All future ICT Hub Strategies / SMART Rwanda plans must consider and include COP. Year 1 focus: Capacity building & build Stakeholder Group | Publish definitions & language based on best global practice relating to COP, the digital environment and child abuse. | NCC to establish and designate a COP expert desk department. Become a member of Safer Internet Day Committee in Rwanda. | Commission a framework for KPIs on policy implementation by sector | 680P Provide training for key institutional actors and enforcement leads; ensure an understanding of COP matters including online risks that result in criminal activity (including online CSA, CSE and trafficking) | Propose amendments if any to legislation in areas identified by gap analysis: a. Cyber Security b. Human Trafficking c. Child Protection d. Penal code e. Children's Rights | Establish clear CSAM definitions -across all harms – in line with ICMEC to feed into definitions in steering group | Introduce a right to the protection of personal data into the constitution or applicable High level legislation | Develop reporting mechanisms and ensure accuracy. Create baseline of data | Identify existing international treaties and protocols | 680P Establish baseline data on existing removal of material, and set targets | Provide training for enforcement and investigation officers in investigation and offender management | Provide COP training at all One Stop Centres. Ensure centres are able to report/provide support to victims | Hold industry roundtable and values-driven conference to reiterate local concerns and requirements. Provide training to Stakeholders in ISPs. | Hold industry roundtable and values-driven conference to reiterate local concerns and requirements. | Hold industry roundtable and child roundtable to discuss issues around safety approaches, tools and software. | 680P Develop school policy on child protection and COP, train to ensure understanding of online risks | Promote positive internet use (e.g. digital literacy, edutainment & educational content schemes) | Develop mandatory COP session(s) to be included in UCR citizenship module, as a blueprint. | Provide training for school head teachers/ teachers on COP issues in schools | Develop a set of key messages and images about COP, establish government webpage, disseminate messages via communications plan | Establish how to reach parents and what information parents need/want to know about COP | 680P Identify key research and evaluation priorities, establish baseline COP data. Coordinate with Ministry of Education to conduct focus groups in schools, to gather COP relevant data. | Support innovation community to develop awareness of social and legal issues | Identify leadership for a singular COP centre of excellence in Rwanda | Identify regional partners to support COP Activities | MINICT Ministry of ICT and Innovation | |
| 2020 | Ensure delivery of implementation plan and KPIs. Year 2 focus: Legal & Regulatory with Industry | Review and update definitions (maintain consistent use of terminology) | Develop COP training for stakeholder groups and COP leads in each sector | Establish baseline information by sector | 680P Develop COP training package for all stakeholders in Justice | Develop programme of legislative upgrade through parliament, including ratification and incorporation of International Protocols | Bring forward a programme to introduce ICMEC, Child Dignity Alliance and Model National Response recommendations | Introduce an updated data protection regulation, with specific protections for children's data. Develop and enforce code of practice to protect children's data in 'data-free' bundle deals | Identify barriers to investigation & prosecution. Conduct annual review of crime reports | Formal adoption of relevant treaties and protocols | 680P Engage with industry to establish protocols for removal of material. Establish dedicated hotline for COP issues | Publish clear guidelines on investigation and offender management across all criminal justice stakeholders. | Train counsellors on COP issues and working with children who have been abused. | Publish safety-by-design standards and guidance for industry. Ensure all mobile subscription bundles and mobiles manufactured in Rwanda adhere to these standards. | Require explicit advertisement notices (e.g. influencer marketing). Investigate implications of children's use of data-free bundle deals and accessibility programmes. | Publish best practise on safety approaches for digital use. | 680P Incorporate balanced COP lessons in primary and secondary school curricula | Introduce fund for edutainment in local languages. Provide digital literacy training programmes for all Rwandan citizens. | Develop COP sessions specific to each profession: a. Teaching b. Computer science c. Social work and health | Provide training for psychologists, psychiatrists and social workers on issues for COP victims | Develop COP sessions for Umuganda, emphasise community support. Raise awareness about One Stop Centres and COP webpage. Raise awareness about services for victims of online violence. | Raise awareness of COP for parent clubs and other local groups (speakers from One Stop Centres and COP leads in schools) | 680P Set up research programme and research fund, identify international partners; develop KPI's. Assess accessibility of internet and ICT devices, provide disaggregated data (by age, gender, location). | Disseminate agreed safety-by-design standards to industry (including a checklist) – see 5.4.4 A&B | Create fund and establish academic attachments to centre of excellence | Engage regional Partners to support COP Activities | MINIJUST Ministry of Justice | |
| 2021 | Ensure delivery of implementation plan and KPIs. Year 3 focus: Education/Public Awareness | Review and update definitions (maintain consistent use of terminology) | Establish Child Protection Leads in every school | Conduct annual review (against KPI frame) | 680P Provide Continued Professional Development for all stakeholders in Justice | Introduce a child focussed online harms bill to address legislative gaps, building on international practice and Rwandan context | Continue programme | Develop guidance for organisations to help them implement the regulations, paying attention to how children's data is processed. Develop capacity building and training within RURA to oversee the new regulations | Develop KPIs for prevention, investigations and prosecution. Develop a database of victims and start matching with global resources | Regional COP conference in Rwanda to create new regional/bilateral agreements and arrangements | 680P Publish protocols for removal of material, make filters available to the public (e.g. ICT managed webpage) | Collect data on COP cases throughout the criminal justice system and develop offender risk assessment and management system | Provide specialist counselling services for children who have experienced online harms | Provide safety software (e.g. Photo DNA) and filters for children, with appropriate default settings | Develop and introduce written standards based on Rwanda values | Require or encourage services to adopt best practise | 680P Identify & train formal child protection leads in every school to enact school's policy. Consider Conduct this training as reward. | Create peer-led programmes for children's safe and positive internet use. | Introduce mandatory COP training sessions for teacher qualification, at primary and secondary school level. | Provide COP training for all health staff and frontline workers in relevant professions (including Entertainment) | Develop specialist messages for hard-to-reach audiences. Assess accessibility in rural areas and enrol rural citizens in digital literacy programs. | Publish guidance for parents and carers that covers: a. Gender b. Early years c. Primary School d. Secondary School | 680P Sponsor research programs by collaborating with COP international partners to access research funds. | Hold Cross-Government Internet Safety Day | Work with Rwanda-based tech entrepreneurs and computer science academics on practical tools for COP | Convene National COP Conference. Identify international partners. | MINEDUC Ministry of Education | |
| 2022 | Ensure delivery of implementation plan and KPIs. Year 4 focus: Response Systems with Health Sectors | Review and update definitions (maintain consistent use of terminology) | Establish Child Protection Leads in health settings / all One Stop Centres | Conduct annual review (against KPI frame) | 680P Ensure that all stakeholders in Justice have received COP training | Review legislative and regulatory landscape | Review and Iterate programme, bring in line with international best practices | Review and improve how children's data is collected and processed by public bodies, paying attention to security and protections required for the publishing of relating statistics and open data. | Review crime reporting and enforcement success rate against established KPIs | Engage with international community to ensure any advances are reflected in established protocols | 680P Ensure protocols are aligned with international best practice (e.g. IWF) | Implement offender management programme, including a focus on the prevention of reoffending | Develop assessment practice to identify online harms. Provide training on recognising harms to wider community | Make region-wide arrangements with providers that meet ethical value standards | Develop clear guidelines for all organisations and services operating in Rwanda | Introduce age-verification schemes; implement flagging systems | 680P Evaluate implementation of COP in schools, by district and by ownership. Set goals to ensure all schools have implemented COP measures, irrespective of ownership. | Co-create edutainment with children and young people. | Incorporate ethics and safety-by-design in all computer degrees and associated qualifications | Provide COP training for all government staff and policy makers | Launch an internet safety media campaign and peer-to-peer campaign, including targeted messages for girls. | 680P Collaborate with COP international partners to access research funds | Innovate safety tools and strategies, develop relevant publications for users | Establish UoR as the regional academic institution on the development of COP cross-sector experience | Convene Regional COP Conference. Engage International Partners | MIGEPROF Ministry of Gender and Family Promotion | | |
| 2023 | Ensure delivery of implementation plan and KPIs. Year 5 focus: Policy Review and Evaluation | Review and update definitions (maintain consistent use of terminology) | Establish Child Protection Leads and community settings | Conduct 3 Year Review (against KPI frame) | 680P Review and Evaluate progress against KPIs; review & iterate training in relation to reports and Steering Committee recommendations | Review and Iterate programme of legislative upgrade | Bring forward review recommendations | Review and Iterate; bring in line with international best practices | Review and Iterate; bring in line with international best practices | Review and Iterate; bring in line with international best practices | 680P Evaluate and Iterate; bring in line with international best practices | Evaluate and Iterate; bring in line with international best practices | Evaluate and Iterate service provision; bring in line with international best practices | Review and Evaluate; identify emerging issues and barriers | Review success and consider if regulation is necessary | Review success and consider if regulation is necessary | 680P Incorporate key research findings into training and teaching qualifications | Run competition for young designers of edutainment and safety measures | Conduct ongoing review and update | Review and Iterate; establish groups with sectors to send needs/ requests to Steering Committee | Evaluate impact and update. | Provide specialist training for new parent groups with children in the early years | 680P Make research findings available to policy-makers and practitioners in a digestible, summarised format. | Assess emerging technology to update industry guidelines | Benchmark findings against international research studies for comparison; highlight specific national issues | Convene International COP Conference | RISA Rwanda Information Society Authority | |
| Authority | Steering Committee | Steering Committee | Stakeholder Group | Stakeholder Group | RISA, NCC | MINIJUST | MINIJUST | MINICT, RISA, RURA | Prosecution and Investigation Authorities (NPPA, RIB, RNP) | MINIJUST, MINICT | MINIJUST | MINIJUST | One Stop Centres | MINICT | MINICT | MINICT | MINEDUC | MINEDUC | University of Rwanda, MINEDUC | University of Rwanda, MINEDUC | MINICT | MIGEPROF | RISA, University of Rwanda | MINICT, RISA | MINICT/University of Rwanda | Steering Committee | | |
| Reports to | Prime Minister and Minister of ICT and Innovation | Minister of ICT and innovation | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | MINISANTE | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Steering Committee | Minister of MINICT | | |

Child Online Protection Communications

COMMUNICATIONS STRATEGY DEVELOPMENT

Key to delivering COP is an understanding of basic concepts of child safeguarding and how they manifest in online situations. The number and range of audiences who need this understanding is very broad, and during the period of policy development it became clear that having messages that could be repeated in all settings and specific messages for particular audiences – would help set the bar for all stakeholders.

Karmarama, a London based creative agency, were asked to devise a set of core COP messages for mass communication in Rwanda. The brief was to inform and educate whilst encouraging the use of digital technology by children.

In coming to the proposed solution, which was warmly received by Rwandan colleagues, they went on a journey that looked at existing campaigns in Rwanda, as well as successful public information and public health campaigns in the UK. One of their key observations, that should be noted for other communication and training communications was that the vast majority of the interface between user and online service has a very simple, ease of use, global style in a few well tested colours. The Karmarama team decided that the images should mirror the aesthetic of the technology that children were accessing in order to look like the thing it was trying to inform them about. As a result, their campaign could work equally in Rwanda and elsewhere.

Three possible brand icons were explored, the first featuring a computer cursor, the second features a person and Wi-Fi symbol, and the third features the African grey parrot (the Einstein of birds). Brand ideas were shared with UK primary school children and representative of the Ministry of ICT and Innovation, Government of Rwanda before further development. The favourite in both groups was brand option three, featuring the African Grey Parrot. This design concept was explored further and multiple ideas of the brand logo were developed (shown in the PowerPoint Slides). The final proposed brand for the COP public awareness campaign is shown here (page 49).

The final 'Get Smart. Use the Internet. Don't let it use you' strap line, ties in with the SMART Rwanda initiative⁴⁵ on the use of smart devices, and the suggestion that using the internet is a skill to be learned rather than an innate quality. The Messages are simple, succinct and instructive. Messages communicate a potential issue and provide a potential solution, e.g. it's safe to open emails from friends but not from strangers, so delete emails from strangers.

Findings from the gap analysis have been instrumental in development of the communications strategy:

- Public awareness materials should not be text-heavy;
- Images help to communicate messages;
- A media campaign (via T.V, radio, billboards, newspapers, government hosted webpage) are effective dissemination routes
- Core COP messages, generated for this campaign, should be presented to the entire Rwandan population during Umuganda⁴⁶
- The public awareness campaign alongside new COP education programmes in schools would support Rwandan children being educated about online safety
- The public awareness campaign alongside community meetings/an active national youth council would ensure that parents and caregivers receive key messages and will therefore be better informed about online risks, to help children navigate the online environment

45 http://www.minecofin.gov.rw/fileadmin/templates/documents/sector_strategic_plan/ICT_SSP_SMART_Rwanda_Master_Plan_pdf

46 <http://www.rgb.rw/index.php?id=37>

KARMARAMA
GOOD WORKS

Child Online Protection: Rwanda
19.03.19

Communication challenges

- Multiple audiences with different perspectives
- Multiple messages for multiple audiences
- Wide range of message types;
- rational & emotional
- detailed & broad brush
- positive & negative
- instruction & persuasion
- Communication idea needs to be capable of being delivered through multiple channel types – media (TV, radio, newspapers), in person, online, in public spaces (posters, healthcare centres, schools), etc.

Need to simplify

Because there are so many audiences we need to start by finding simple truth as a starting point from which all other communication can flow

Brands are how we wrap emotional & rational associations into a single, simple package – Child Online Protection must be a brand

Build up the campaign in layers

- Consider the right shape for the communications plan
- Sequencing the campaign – not everything all at once
- Use different contexts/media so each plays to its strengths
- Get the right message for the right context
- Consider if different stakeholders should speak in a different voice

However many voices, however many contexts, whatever the media; the message remains the same.

The communications approach

Create a common cause – to keep children safe.

Create awareness of failure to act – harm to children.

Establish a positive but urgent voice – straightforward, helpful, clear.

Create a timeline over which to deliver communications.

Create a distinctive verbal and visual vocabulary.

Make available images and messages so that others can easily incorporate into their own tools, messages and programmes.

A framework for messaging

AGITATE

Get people to pay attention to the problem

EDUCATE

Give people the information they need to understand what they need to do

AFFILIATE

Give people the tools they need to understand and adopt new behaviours

The right message will contain
both silver lining and cloud

UPSIDE

Persuasive & emotional
Displaying ideal behaviours

Instructional & factual
Warning of dangers

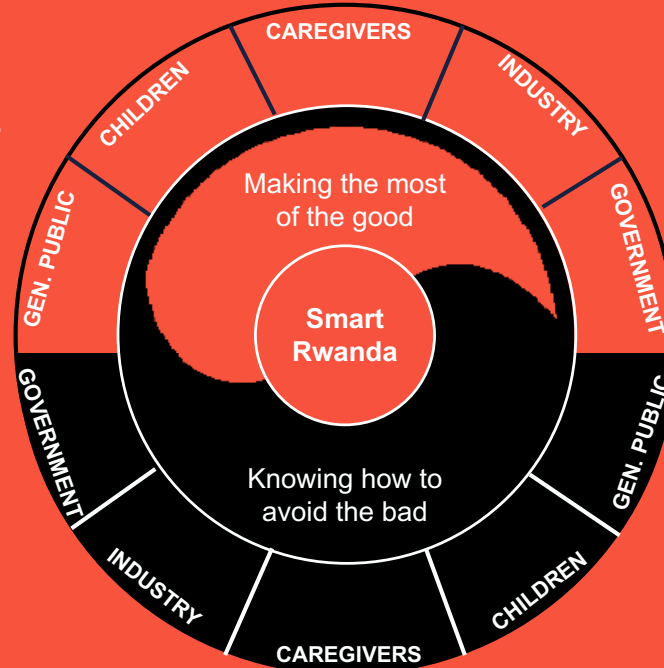
DOWNSIDE

The task

1. Create a memorable and visually distinctive brand that will be the voice of an ongoing national campaign to promote Child Online Protection in Rwanda
2. Create the idea that can sit at the heart of the campaign – an idea that can carry both positive messages and warnings



Audience segments



Messaging by segment (illustrative)

General Public



Children



Caregivers



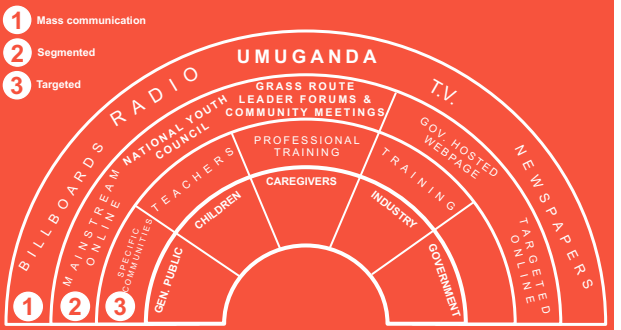
Industry

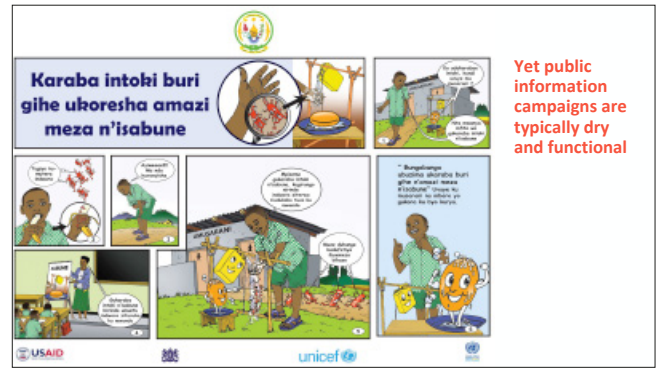


Government



Bringing the message to life in all the right places





Staying safe should be seen as an intrinsic part of this brave new digital world

Not an attempt by traditionalists to ration or neuter it

The brand should feel native to the Global, borderless internet

Not parochially Rwandan

This is global best practice

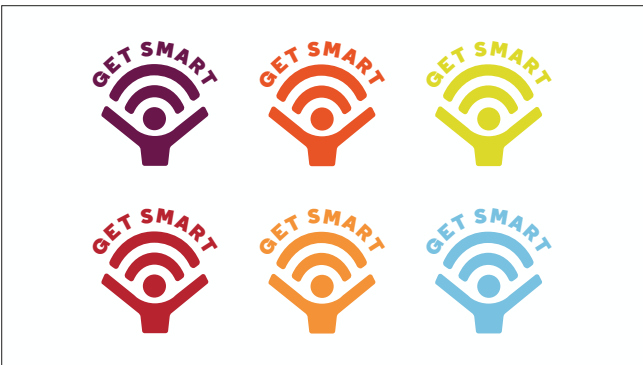
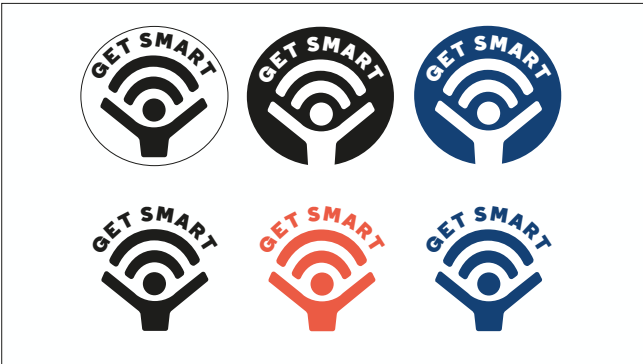
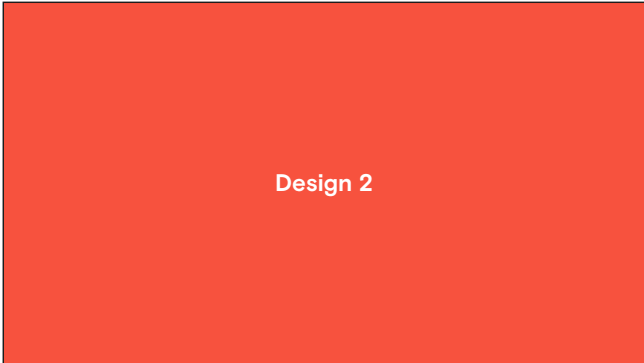
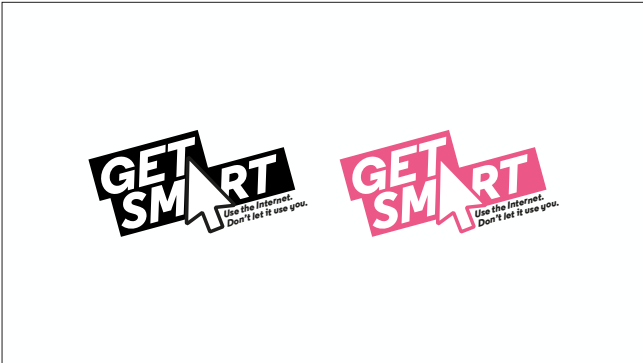
Not 'internet lite' for those not yet ready for the real thing

It's smart to make the most of the internet,


but smarter still to do it safely

Get Smart
Use the Internet. Don't let it use you.

Nobody is born smart. You have to get smart. You do that by learning, by asking questions and by finding answers. It's the same when you use the internet for the first time. You're not born knowing how to use it, you have to learn. That's why we've created 'Get Smart.' It's here to tell you everything you want to know about the internet. That way, you and everyone else can Get Smart.



Final design



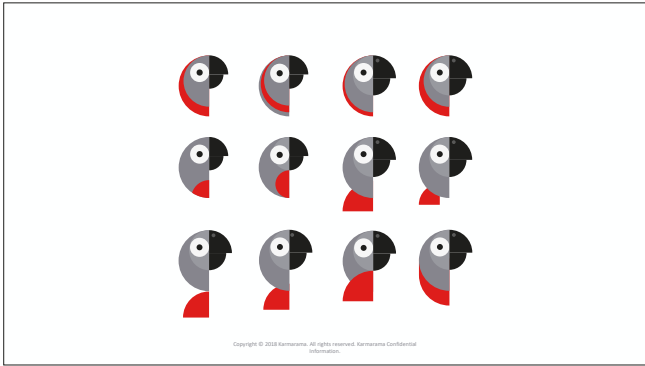
African Grey Parrot

Known as the Einsteins of the parrot world, African Greys are highly intelligent.

Studies have shown that the birds possess abstract, inferential reasoning abilities.


They appear to have some understanding of causality and use it to reason about the world.

African greys also show their smarts with their counting abilities and vocalization skills.





Adcepts

Opening an email from a friend.




Simple.

Deleting an email from a stranger.




Smart.

Opening an email from a friend.




SIMPLE

Deleting an email from a stranger.




SMART

Opening an email from a friend



Simple

Deleting an email from a stranger



Smart

Use the internet. Don't let it use you.

NB The above are adcepts to show how the messaging & branding might work in practice, not proposed finalised designs

**Opening an email from a friend. Simple.
Deleting an email from a stranger. Smart.**

Find out more at getsmart.rw

**Sharing a photo of you and your friends. Simple.
Asking them if it's okay to share the photo. Smart.**

Find out how at getsmart.rw

**Buying things online. Simple.
Keeping your bank details secret. Smart.**

Find out how at getsmart.rw

**Watching a video online. Simple.
Reporting an offensive video. Smart.**

Seen something upsetting? Call xxx to report it
or find out more at getsmart.rw

Conclusion

It was a privilege to work in Rwanda on the development of a comprehensive COP policy. The institutions and individuals that we engaged with had a palpable appetite to implement COP as a prerequisite for children's safety as the country embraces deeper penetration of digital technologies in everyday life.

Many of the concerns of Rwandan stakeholders reflected those of the global community; the wide distribution of inappropriate content, insufficient protections from predators, failure to report or take-down CSA material, misinformation and disinformation (false narratives), technology distracting children from essential and/or beneficial familial, social or educational activities – and issues around gender inequality and discrimination. Other concerns were more specific to the Rwandan context, for example, ensuring local content (language and subject), maintaining Rwandan values, infrastructural capacity, affordability and literacy (both digital and written).

This same split was apparent when considering implementation – whilst most policy areas of COP are common across jurisdictions, the road to implementation depends on institutional capacity, access to particular skills and specialisations, sufficient infrastructure and adequate resources to implement across a complex landscape.

Key to ensuring the success of Rwanda's newly adopted COP policy is to create the conditions in which it can be implemented. For this, continued leadership, institutional capacity building, robust measurement and evaluation, as well as significant commitments from all stakeholders, across government, private sector, NGO's, civil society and the international community – are required.

Child online protection does not sit in a vacuum, and as access to digital technologies becomes more widespread it will increasingly be a component of a Rwandan child's everyday life. Much of Rwanda's COP policy is therefore focused on prevention. Safety-by-design, filters, data protection, training, education, public awareness, and corporate responsibility – each of these components offer thoughtful consideration of children's needs, before harm happens. Life, both on and off line, cannot be entirely risk free, which means that even whilst emphasising the need to marshal all preventative approaches, there will always be a need for robust legal frameworks, reporting mechanisms, enforcement, victim support and evidence-based systems to deal with those who exploit or harm children across each of the identified areas of concern – content, contact, conduct and contract (commercial) harms.

Many of the detailed recommendations are embedded in the policy and implementation plan itself, but it's worth noting that whilst some jurisdictions have a highly developed infrastructure and others are still at the very beginning of their journey to connectivity, there is no country that has yet fully implemented a comprehensive COP strategy across each of the 8 policy areas and their component parts. Rwanda should be justly proud that they have set an ambitious path to delivering comprehensive child online safety, and in doing so, shown the way for nation states across the globe.

Contributors

AUTHORS

Baroness Beeban Kidron

Beeban Kidron, Baroness Kidron OBE is an English film director, producer, children's rights campaigner and member of the UK House of Lords.

She is the Founder and Chair of 5Rights Foundation, a thought leader in wherever children interact with the digital world, and a frequent speaker on data protection, AI and how childhood could and should be better supported in the 21st Century.

Her previous career as a film director spanned 30 years, directing a wide range of commercial movies and hard-hitting documentaries, including an adaptation of Jeanette Winterson's autobiographical novel *Oranges Are Not the Only Fruit*; *Bridget Jones: The Edge of Reason*; the cult classic *Too Wong Foo, Thanks for Everything! Julie Newmar*; *Sex, Death and the Gods* and *InRealLife*.

Baroness Kidron is the joint founder of the educational charity Into Film, which uses film to educate children in after-school clubs in the United Kingdom.

Professor Julia Davidson, Principal Investigator

Julia Davidson is Professor of Criminology in the Department of Law and Criminology at the University of East London and is Co-Director of International Centre for Cyber Research at the University of East London. She is one of the UK's foremost experts on policy, practice and offending in online offending, with a specific focus on online victimisation and cybercrime. She plays an active role in key national committees such as the UK Council for Internet Safety (she chairs the Evidence Group) and provides expert advice to international organizations such as UNICEF, Europol, the US Sentencing Commission, the US Department of Justice and the United Nations (UN) ITU. She is a member of the Interpol Specialist Crimes against Children Group and of the Europol EC3 Expert Academic Advisory Group. She has recently joined the UK Inquiry into Institutional Child Sexual Abuse. As Chair of the Ethics Committee, she recently joined the Board of the Hague Justice Portal (www.haguejusticeportal.net/index.php?id=13397_). She has directed a considerable amount of national and international research spanning 30 years.

Recent examples include a European Commission-funded ISEC study spanning four EU countries exploring industry and policing practice in the prevention of online child abuse (see www.euchildsafetyonlineproject.com), and a study exploring young people's pathways into hacking undertaken in collaboration with the Europol Cybercrime Centre (EC3). She has also acted as an advisor on child internet safety to governments and practitioners in the MENA region, Africa and South America (Suriname), and has aided the Kingdom of Bahrain in developing a national Child Internet Safety Framework (2010, 2016). She is currently co-leading a project funded by end violence against End Violence Against Children focusing on child online protection in Rwanda. Julia has worked extensively with the media and has published widely on abuse and internet safety, and has written many academic books and articles.

She has a PhD in Criminal Justice Policy from the London School of Economics and Political Science (LSE), and was made Honorary Research Fellow at Royal Holloway University of London in May 2010. She is a Fellow of the UK Higher Education Academy. Julia provides regular expert advice on criminal justice issues to the media, and has recently worked on documentaries for the BBC and ITN. She has worked with ITV Evening News, the ITV News Channel, BBC News Channel, BBC Radio Four Woman's Hour, BBC Five Live Radio, BBC 2, BBC Northern Ireland, C4 and Sky News.

Kirsty Phillips, Project Coordinator

Kirsty Phillips is doctoral researcher at Birkbeck, University of London. PhD

themes and current research involve Judgement and Decision Making, Bayesian Inference, Rationality and Evaluation of Eyewitness Testimony. Work undertaken as part of this PhD has been presented at and published by the Cognitive Science Society. Kirsty has previously worked as a research assistant at Birkbeck, for the Bayesian Argumentation via Delphi (BARD) project, in collaboration with Monash University, University College London and University of Strathclyde. The BARD project was part of the Crowdsourcing Evidence, Argumentation, Thinking and Evaluation (CREATE) program and funded by Intelligence Advanced Research Projects Activity (IARPA), of the Office of the Director of National Intelligence. Kirsty graduated University College London with a Distinction in Research Methods in Psychology MSc and Warwick University with a First Class degree in Psychology, BSc (with Honours).

PROJECT CONSULTANTS

John Carr*

John Carr OBE, was a founding Director of the Internet Watch Foundation in 1996/97 and was a member of the UK Government's principal co-ordinating body for online child protection policies from 2001 until 2018. He is a Visiting Senior Fellow at London School of Economics and Political Science. He is a former Vice President of MySpace and former Board Member of Microsoft's Policy Board for Europe, the Middle East and Africa. He is currently Senior Technical Adviser to ECPAT International, a global NGO based in Thailand and Technical Adviser, European NGO Alliance for Child Safety Online, which is administered by Save the Children Italy. He is also a Member of Advisory Council, Beyond Borders (Canada) and a consultant to Council of Europe and United Nations (ITU).

Kathryn Corrick*

Kathryn is founding partner of Corrick, Wales & Partners LLP (www.corrickwales.com), who work with organisations to implement data protection and privacy regulations. With a keen interest in innovating responsibly and the impact of technology on society, Kathryn brings together experience of digital technology development, communications and change management with a practical understanding of public policy and compliance. She works to enable organisations to consider business, regulatory and technology requirements and to build cultures for sustainable change. She co-founded democracy platform Represent.me, was head of learning and content at the Open Data Institute from 2012-2015, and was online manager for the New Statesman until 2006.

Richard Graham*

Dr Richard Graham is a Consultant Child & Adolescent Psychiatrist, and former Clinical Director of the Adolescent Directorate at the Tavistock Clinic. He is currently Clinical Lead for Good Thinking: London's Digital Mental Well-being Service (<https://www.good-thinking.uk>), and Director of Trust and Well-being at TalkLife (<https://talklife.co>). Over the last decade, his work has centred on the impact of technology on development and health. In 2010 he launched the UK's first Technology Addiction Service for young people at Nightingale Hospital in London. In June 2016, he was appointed the Executive Board of the UK Council for Child Internet Safety (UKCCIS is the British Government's principal advisory body for online safety and security for children and young people) and Co-Chairs the Digital Resilience Working Group. He also works with the BBC, as Digital Well-being Consultant to the Own It App Project (<https://www.bbc.co.uk/programmes/p074q3jc>).

Anna Gekoski*

Dr Anna Gekoski specialises in qualitative trauma focused research, with over ten years' experience conducting research in the areas of forensic psychology, criminology, and mental health. Her research interests include cybercrime, child sexual abuse, secondary victimisation, rape, homicide, victims of crime, hate crime, mental health, and ethical issues in trauma focused research. Anna has worked on trauma focused research projects, with teams of researchers from Middlesex University and the University of East London, for the Office of the Children's Commissioner, the British Transport Police, the Department for Transport, the Ministry of Justice, and the Department for Digital, Culture, Media and Sport. In her various roles as an investigator, senior investigator, research fellow, project manager, and quality and assurance overseer, she has been involved in conducting empirical research studies, literature reviews and Rapid Evidence Assessments on child sexual abuse, rape, youth offending, unwanted sexual behaviour on public transport, and online harms including hate crime, revenge pornography, image based sexual abuse, and cyberharassment.

Anna is also Director of Research at independent research consultancy BroomelGekoski and a research associate at the University of Central Lancashire, working on projects around mental health, wellbeing, loneliness and social networks, on projects funded by clinical commissioning groups, local councils, and mental health charities. Before retraining in forensic psychology, Anna was a national newspaper journalist for ten years, working as a news reporter specialising in crime. In addition to writing for numerous national newspapers, she has published research in highly ranked peer-reviewed academic journals, written review chapters for edited books, co-authored reports for government bodies and NGOs, written for magazines for psychology and sociology students, and authored three popular non-fiction books in the areas of criminology and psychology.

Karl Hopwood*

Karl Hopwood is an independent online safety expert. He is a member of UKCIS (UK Council for Internet Safety) and sits on the UKCIS evidence group and the UKCIS education group as well as on the advisory board for the UK Safer Internet Centre and the education advisory board for CEOP. He also sits on Twitter's trust and safety council where he represents the Insafe network. Karl has worked for a number of key players in the UK and abroad including CEOP (Child Exploitation and Online Protection Centre), BECTA (British Educational and Communications Technology Agency), the European Commission, the UN and several Local Authorities within the UK and in Europe. As an ex primary head teacher, he continues to work closely in schools across Europe with children, young people, parents and teachers to develop safer online behaviours and the promotion of digital literacy. Karl has been employed for the last 12 years as an in-house consultant for INSAFE which is the coordinating node of the EU Better Internet for Kids programme where he is responsible for the coordination of safer internet helplines across Europe. Karl is the Chair of the Board of Trustees of the Marie Collins Foundation, a charity which supports young people who have been sexually abused and exploited online and is also a trustee of Childnet International. He is currently part of a team working on child protection policy development in Rwanda in collaboration with 5Rights.

Karmarama

Karmarama is the UK's most progressive creative agency, part of Accenture Interactive, working across advertising, PR, data-driven communications, mobile platforms and products, digital and innovation. The agency is known for its ability to blend creativity, digital and data, to help brands better engage with consumers, or as Karmarama calls it - Connected Creativity. It is one of the most effective agencies in the UK and has won the DMA Grand Prix for the last two

successive years, in 2017 for its work for the Army. It was again the highest ranked creative agency in the Sunday Times Top 100 Companies to Work For in 2019.

Chief Executive Officer: Ben Bilboul
Chief Creative Officer: Nik Studzinski
Strategy lead: Will Collins
Account Director: Amanda Wright

Creative Director: Ed Robinson
Creative: Paul Pearson
Agency Producer: Cassy Bhairo
Head of Design: Simon Wakeman
Designer: Hannah Woodall

Elena Martellozzo*

Dr Elena Martellozzo is one of the leading experts on online child safety. Dr Martellozzo has worked extensively with children, serious offenders and practitioners. She has conducted research for organisations such as the Centre of Expertise for Child Sexual Abuse, the Internet Watch Foundation, the NSPCC, the Children Commissioner for England, the Kingdom of Bahrain, the Exploitation and Online Protection Centre.

The findings of her research on online abuse and online safety are helping to inform police and other key agencies' strategies and practice.

She has published work on protecting children on the net, the risk, control and state surveillance of internet sex offenders and how sex offenders use the internet.

For more information about Dr Martellozzo please see this link:

<http://www.mdx.ac.uk/about-us/our-people/staff-directory/martellozzo-elena>

She can be contacted here: e.martellozzo@mdx.ac.uk

Abhilash Nair*

Abhilash Nair is Senior Lecturer in Internet Law at Aston University, Birmingham. He is a world-leading expert on online child safety laws, and has advised various international and national bodies on regulating illegal content on the internet, online child sexual abuse material, internet pornography, and content-related cybercrime. He has published widely on aspects of internet law and regulation, and has been a regular speaker at international conferences and seminars. Abhilash's recent research monograph titled 'The Regulation of Internet Pornography: Issues and Challenges' (Routledge) examines how the internet has necessitated a fundamental change in the regulation of pornography.

Abhilash is the Editor in Chief of the European Journal of Law and Technology, one of the oldest open access law journals in Europe (formerly published as JILT). In addition, he serves as the Deputy Editor of the International Review of Law, Computers and Technology (Routledge), and an Associate Editor of the European Journal of Current Legal Issues. Abhilash is Secretary of the British and Irish Law, Education and Technology Association and has served as a member of the Technology Law and Practice Committee of the Law Society of Scotland. Abhilash is a member of the Evidence Working Group of the UK Council for Internet Safety (UKCIS).

***Project consultants were also members of the UK Expert Group**

UK EXPERT GROUP MEMBERS

| | |
|--------------------------|--|
| Jonathan Baggaley | Chief Executive, PSHE Association |
| Emran Mian | Director General (interim), Higher Education and Further Education |
| Chris Bonell | Professor of Public Health Sociology LSHE |
| Adam Kinsley | Director of Policy, Sky |
| Joanna R Adler | Professor, University of Hertfordshire |
| Ben Terrett | Designer and CEO at Public Digital |
| Emily Middleton | Principal Consultant at Public Digital |
| Gareth Edwards | Norfolk Constabulary |
| Jen Persson | Director, defenddigitalme |
| Superintendent | Head of International Development and Innovation Unit, Police Scotland |
| John Wyllie | Deputy Chief Constable, Police Scotland |
| DCC Will Kerr | NHS Improvement / NHS, Baroness Harding of Winscombe |
| Dido Harding | |
| Jenny Jones | Director, Public Policy at GSMA |

RWANDAN STAKEHOLDER GROUP

Special thanks is given to the University of Rwanda in facilitating this research project, in particular to Professor Philip Cotton, Vice-Chancellor, University of Rwanda, and Michael Tusiime, Lecturer of Computer Engineering, University of Rwanda.

A list of stakeholders already actively involved in the COP Project:

MINISTRY OF ICT AND INNOVATION (MINICT)

| | |
|-----------------------------|--|
| Gordon Kalema | Director General Digital Transformation |
| Victor Muvunyi | E-transaction & Data revolution specialist |
| Paul Ndungutse | Technical Advisor |
| Elysee Tuyishime | Public Relations officer |
| Uzayisenga Seraphine | Administration Liaison Officer |

RWANDA INFORMATION SOCIETY AGENCY (RISA)

| | |
|---------------------------------|--|
| Josephine Nyiranzeyimana | Government Chief Information Officer |
| Sylvie Ndanga | Social Cluster Digitalization expert |
| Anatole Gahongayire | Ag. Division Manager Public Key Infrastructure |

MINISTRY OF JUSTICE (MINIJUST)

| | |
|----------------------------|-------------------------------|
| Mutagoma Damas | Advisor to the State minister |
| Umurungi Providence | Head of Department |

RWANDA INVESTIGATION BUREAU (RIB)

Nshimiyimana Alphonse Anti-Gender Based Violence Investigator

RWANDA NATIONAL POLICE (RNP)

Mwenzu Gorethe

Anita Nanyonga Kamiyati Officer in charge of GBV and Child Protection

MINISTRY OF GENDER AND FAMILY PROMOTION (MIGEPROF)

Minister Solina Nyirahabimana Minister

NATIONAL CHILD COUNCIL (NCC)

Bernadine Mahoro ICT officer

Dr Claudine UweraUweraUwera Executive Secretary

Lambert Hategekimana Child Rights Protection and Promotion Officer

UNIVERSITY OF RWANDA (UOR)

Prof. Philip Cotton OBE Vice Chancellor

Michael Tusiime Lecturer -- Computer Engineering

Dr Gaurav Bajpai Head of Computer Engineering & AG CIO

Serugo Jean Baptiste Lecturer - School of Law

Uwihangana Consolee Assistant Lecturer - Social Science/ Social Work

Darius Gishoma Senior Lecturer - Mental Health

Dr Celestin Hategekimana Senior Lecturer - CGS

Stakeholder interviewees ranged from lawyers, child and women's rights advocates, teachers, government and academic staff.

OTHER IDENTIFIED POTENTIAL PARTNERS, TO INCREASE NETWORK:

ICT

- Representative(s) from coding schools
- Cyber security organisation: Cyberteq – Kigali⁴⁷
- Improving access: The Ministry of Infrastructure (MININFRA) www.mininfra.gov.rw
- Reporting ICT access: Rwanda Utilities Regulatory Authority <https://rura.rw>
- Seek to become a member of Safer Internet Day Committee in Rwanda (<https://www.saferinternetday.org/web/rwanda/sid>)
- Industry partners:
- Rwanda Smartphone Factory
- Rwanda's Innovation City
- Developers of smartphones (MaraPhones), Android Oreo (OS optimized for apps made for African Market)
- Developers of apps
- Service Providers
- GSMA Sub-Saharan Africa

47 Cyberteq is an innovative Information and Communication Technology Consulting Company. In the era of digitalization, Cyberteq enables its customers to take full advantage of the latest digital technologies and networks in a secure manner." Cyberteq has previously run cyber awareness campaigns in schools in Kigali. Source: <http://rwandainspirer.com/2018/01/28/why-children-should-be-aware-of-cyber-crimes/>

48 "Coalition Umwana Ku Isonga brings together different child rights focused organisations for the purpose of networking and alliance building with a mandate to advocate on child rights related issues, assess and report on the implementation of child related treaties and conventions especially the United Nations Child Rights Convention (CRC) and the African Charter on the Rights and Welfare of the Child (ACRWC)." Previously hosted by HAGURUKA and CLADHO.

49 "HAURUKA has been 'standing up' (Haguruka means 'stand up' in Kinyarwanda) for the rights of women and children. Our vision is to create a society where women and children can enjoy equal rights and reach their full potential. Our advocacy efforts have influenced several national law reforms, the proposal of new laws, and the formulation of policies in favour of women and children. We bring our legal expertise to various regional centres in provinces across Rwanda, with our headquarters located in Kigali Our team provides vital access to services for vulnerable women and children, receiving referral cases from institutions such as the National Police, the National Prosecution Services, Courts and the Local Government."

50 "CLADHO is a well-established human rights umbrella organization in Rwanda, active in the area of human rights promotion, economic governance, right to socio protection, right to education and citizen participation. It was founded in May 1993 with the mission to protect, defend and promote human rights. It focuses on social and economic rights, especially in child protection, social security, labor law, budget analysis and advocacy. CLADHO aims at empowering citizens and civil society of Rwanda to participate and influence effectively public policies formulation and implementations in general. CLADHO is a network of 12 human rights organizations (AVP, CSC, AERG, TI-RW, ARDHO, MPEDH, RWAMREC, AJPRODHO, LIPRODHOR, BENIMPUHWE, KANYARWANDA, NEVER AGAIN RWANDA) that participate in programs and projects implementation in Rwanda."

LAW ENFORCEMENT

- Rwanda National Computer Security and Incident Response Team (Rw-CSIRT) <http://www.rw-csirt.rw>
- Rwanda INTERPOL National Central Bureau (NCB) – Kigali

EDUCATION

- The Ministry of Education (MINEDUC), www.mineduc.gov.rw
- National Youth Council <https://nyc.gov.rw>
- Messaging: The Ministry of Local Government (MINALOC), www.minaloc.gov.rw

OTHER

- Health: The Ministry of Health (MINISANTE) www.moh.gov.rw,
- Financial security: The Ministry of Finance and Economic Planning (MINECOFIN), www.minecofin.gov.rw
- E-Agriculture: The Ministry of Agriculture and Animal Resources (MINAGRI), www.minagri.gov.rw

CHILD, GENDER AND FAMILY

- The Ministry of Youth (MINIYOUTH) www.miniyouth.gov.rw
- National Youth Council <https://nyc.gov.rw>
- Children's (and Women's) rights organizations:
- Coalition Umwana Ku Isonga⁴⁸
- HAGURUKA⁴⁹ – 2018 Annual Report
- Research on Teen Mothers
- CLADHO⁵⁰ – 2017 Annual Report
- Report on Teenage Pregnancy
- The Ministry of Sport and Cultural (MINISPOC) www.minisporc.gov.rw

Further Resources

Resource Directory COP Policy Document

During the course of policy development, a great deal of sources were consulted. This directory follows the eight Policy Areas of the Rwanda Child Online Policy document – some sources may correspond with more than one area, but appear at the first mention. Where there are hyperlinks in the text, the same information is provided as footnotes.

This is not a comprehensive directory – COP is a fast-changing area, and the directory offers a snapshot of resources and examples of best practice currently available. The document also cites many UK examples that are both a reflection of the UK based expert group and the UK's leadership in this policy area. This document was created at the specific request of Rwandan experts and stakeholders and should be read in conjunction with the five-year implementation plan. The implementation plan is designed to be progressive; each subsequent year is dependent upon effective completion of the year before.

ABBREVIATIONS

| Acronym | Expansion |
|----------------|--|
| 4G LTE | 4G Long Term Evolution |
| ACRWC | African Charter on the Rights and Welfare of the Child |
| AYC | African Youth Charter |
| CAM | Child Abuse Material |
| COP | Child Online Protection |
| COP | Child Online Protection |
| CRC | Convention on the Rights of the Child |
| CSA | Child Sexual Abuse |
| CSA | Child Sexual Abuse |
| CSAM | Child Sexual Abuse Material |
| CSE | Child Sexual Exploitation |
| EICV | Integrated Household and Living Conditions Survey |
| GBV | Gender Based Violence |
| GCA | Global Cybersecurity Agenda |
| ICT | Information and Communications Technology |
| ICT(s) | Information and Communication Technology(ies) |
| ISP | Internet Service Provider |
| ISP | Internet Service Provider |
| ITU | International Telecommunication Union |
| ITU | International Telecommunication Union |
| KPIs | Key Performance Indicators |
| MIGEPROF | Ministry of Gender and Family Promotion |
| MINEDUC | Ministry of Education |
| MINICT | Ministry of ICT and Innovation |
| MINICT | Ministry of ICT and Innovation |
| MINJUST | Ministry of Justice |

5.4.1 POLICY AREA: COP INSTITUTIONAL CAPACITY

The Year 1 activities listed in the implementation plan under this policy area focus on awareness and capacity building, and include the development of a stakeholder network, publishing a COP language and definitions manual, and providing training to those in the stakeholder network.

IMPROVING COP KNOWLEDGE AND RESOURCES: CROSS SECTOR

Recent UK Developments

- UK Government: Online Harms White Paper⁵¹, Published April 2019
- ICO's (Information Commissioners Office) Age Appropriate Design Code, Consultation Document⁵², published April 2019
- 5Rights Foundation's response to the ICO here⁵³.
- Responses from other organisations⁵⁴

Children's Rights

- United Nations Children's Fund (UNICEF) is internationally renowned for its work on children's rights:
 - The 2030 Agenda for Sustainable Development⁵⁵
 - Convention on the Rights of the Child⁵⁶
 - UNICEF's information on ENDViolence⁵⁷
 - ENDViolence Online⁵⁸
- End Violence Against Children (EVAC) is a global partnership, from organizations to children themselves, with the sole purpose of ending violence against all children
- Save the Children is active in 120 countries, and is committed to improving the welfare of children internationally and protecting children from harm. Save the Children's 2017 Annual Report⁵⁹
- 5Rights Foundation takes the existing rights of children and young people (under 18), and articulates them for the digital world.

Child Protection/Safeguarding

- Child Protection:
 - UNICEF believe that every child has the right to grow up in a safe and inclusive environment, working with partners around the world to promote policies and expand access to services that protect all children. Here is their website that provides guidance on Child Protection⁶⁰
 - Child Exploitation and Online Protection Centre (CEOP) produced a 2010 report⁶¹ that speaks to Child Protection in the online environment
 - Every Child Protected Against Trafficking (ECPAT) UK's Child and Young People Policy⁶²
 - International Centre for Missing and Exploited Children's (ICMEC) Child Protection Policies and Procedures⁶³
- Safeguarding:
 - UK HM Government, Working Together to Safeguard Children provides a guide (2018 Report⁶⁴) to inter-agency working to safeguard and promote the welfare of children
 - From the perspective of service provision, the Care Quality Commission (CQC) provided a guide (2015 Report⁶⁵) for the safeguarding of children and adults
 - London Child Protection Procedures and Practice Guidance⁶⁶

51 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

52 <https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf>

53 https://5rightsfoundation.com/static/5Rights_Response_IC_Call_for_Evidence_v2.pdf

54 <https://ico.org.uk/about-the-ico/responses-to-the-call-for-evidence-on-the-age-appropriate-design-code/>

55 <https://www.unicef.org/agenda2030/>

56 https://www.unicef.org/crc/index_30160.html

57 <https://www.unicef.org/end-violence>

58 <https://www.unicef.org/endviolence/endviolenceonline/>

59 https://www.savethechildren.net/sites/default/files/libraries/Save%20the%20Children%20Annual%20Review%202017_0.pdf

60 <https://www.unicef.org/what-we-do#protection>

61 <https://dera.ioe.ac.uk/10569/1/7785.pdf>

62 <https://www.ecpat.org.uk/Handlers/Download.ashx?IDMF=270fed66-1404-4f6c-8cf3-7caeabbdb139>

63 <https://www.icmec.org/education-portal/child-protection/>

64 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779401/Working_Together_to_Safeguard_Children.pdf

65 https://www.cqc.org.uk/sites/default/files/20150710_CQC_New_Safeguarding_Statement.pdf

66 <http://www.londoncp.co.uk/>

Children's use of internet (research and reports)

A recent UNICEF report (State of the World's Children 2017: Children in the Digital World), provides a comprehensive overview of internet access, the benefits and harms associated with online access, how use of ICT is impacting childhood, and recommendations as to how the private sector can positively influence children's online environment.

A recent 2017 Report⁶⁷ (Children's online activities, risks and safety: A literature review) from the UK Council for Child Internet Safety (UKCCIS) provides a comprehensive overview of research in relation to access, children's use of internet, various potential online harms and safeguarding initiatives. One of the authors, Professor Julia Davidson, also edited a 2011 Book⁶⁸, that reviews research and policy in relation to internet child abuse.

The Centre for Justice and Crime Prevention (CJCP) and UNICEF South Africa commissioned a Research⁶⁹ Report (Connected Dot Com: Young People's Navigation of Online Risks), to review online access, online benefits and harms, and children's responses to harms, in South Africa.

A recent UNICEF report⁷⁰ examined Child Online Protection in India, analysing how the rapid increase in mobile ownership and corresponding access to internet may impact the children of India.

Training Materials

The above resources can form the basis of training materials and are necessary for those working in any capacity in relation to COP, however to support the delivery of COP awareness project consultant Karl Hopwood, has provided guidance on what would be required to build a COP training outline for educators/schools (see Appendix B). This guidance, alongside the COP presentation and the resources listed within this document will serve as a basis to develop a COP lessons for (1) the Citizenship Module at the University of Rwanda and (2) professional training in COP.

The International Telecommunications Union (ITU) has published Guidelines for Policy Makers on Child Online Protection⁷¹, and should be reviewed by the steering committee.

67 https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf

68 <https://www.routledge.com/Internet-Child-Abuse-Current-Research-and-Policy-1st-Edition/Davidson-Gottschalk/p/book/9780415559805>

69 https://www.unicef.org/csr/files/UNICEF_South_Africa_Connected_Dot_Com_research.pdf

70 https://www.icmec.org/wp-content/uploads/2016/09/UNICEF-Child-Protection-Online-India-pub_doc115-1.pdf

71 <https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf>

72 <https://www.itu.int/en/ITU-D/Pages/Regional-Presence.aspx>

73 <https://www.itu.int/en/cop/Pages/guidelines.aspx>

74 <https://www.itu.int/en/cop/Documents/profiles/rwanda.pdf>

75 <http://luxembourgguidelines.org/english-version/>

76 <https://www.icmec.org/wp-content/uploads/2018/08/2017-Annual-Report-Final-Digital.pdf>

77 <https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf>

78 <https://www.icmec.org/research-library/>

79 <https://www.icmec.org/joint-program/>

80 <https://www.icmec.org/resources/glossary/>

81 <https://www.getsafeonline.org/jargon-buster/>

82 https://www.icmec.org/wp-content/uploads/2016/09/UNICEF-Child-Protection-Online-India-pub_doc115-1.pdf

- ITU : COP Initiative⁷²
- ITU : COP Guidelines⁷³
- ITU : Rwanda Country Profile⁷⁴

See APPENDIX A: COP MODULE OUTLINE FOR TEACHERS AND EDUCATORS

COP Language & Definitions

- Language and Definitions in relation to online crimes: International Centre for Missing and Exploited Children (ICMEC) & Luxembourg Guidelines⁷⁵
 - ICMEC : 2017 Annual Report⁷⁶
 - ICMEC : CSAM: Model Legislation & Global Review 2018⁷⁷
 - ICMEC : Research Library⁷⁸
 - ICMEC : Model National Response⁷⁹
 - ICMEC : Glossary⁸⁰
- Language and Definitions in relation to online safety and information security: Get Safe Online Jargon Buster⁸¹
- An example of such a glossary of terms can be found in this UNICEF publication: Child Online Protection in India⁸²
- Terminology Guidelines For The Protection Of Children From Sexual

See Appendix C: Terminology Guidelines for COP.

BUILDING A STAKEHOLDER NETWORK

Examples of COP networks

The below examples/resources will be instructive for building a stakeholder network, as well as this guidance⁸³ to building communities of practice. We note that for a stakeholder network to be effective it must have the full support of sector leaders and commitment to cross disciplinary working in a way that each member fulfils their responsibilities.

Steering Committees and Networks:

- UK Council for Internet Safety (UKCIS) Board (Mission Statement⁸⁴)
- WePROTECT Board
 - WePROTECT Advisory Board⁸⁵
 - WePROTECT: Events Page⁸⁶
 - International: ICMEC
 - International: Child Rights Connect
 - Child Rights Connect : 2017 Annual Report⁸⁷
 - International: ECPAT
 - Europe: EUROPOL
 - UK Network: UK Council for Internet Safety (UKCIS)
 - Commonwealth Telecommunications Organisation (CTO)
 - CTO : Cyber Security Programme⁸⁸
- Academic/Research networks
 - UKCIS Evidence Group (Chaired by Prof Julia Davidson) (webpage⁸⁹)
 - UNICEF Innocenti Research Centre
 - Innocenti Research Centre: Children’s Rights Governance⁹⁰
 - Innocenti Research Centre: Children’s Rights in the Digital Age⁹¹
 - Global Kids Online
 - Global Kids Online Project Members⁹²
 - Digitally Connected

83 <https://wenger-trayner.com/introduction-to-communities-of-practice/>

84 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/550887/UKCCISExecutiveBoardTermsOfReferenceJune2016.pdf

85 <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5783df4d15d5dbb3d92c7e95/1468260174098/WePROTECT+Advisory+Board+Terms+of+Reference.pdf>

86 <https://www.weprotect.org/events>

87 https://www.childrightsconnect.org/wp-content/uploads/2018/04/Annual_Report_2017.pdf?x37799

88 <https://cto.int/strategic-goals/cybersecurity/>

89 <https://www.saferinternet.org.uk/research>

90 <https://www.unicef-irc.org/research/child-rights-governance/>

91 <https://www.unicef-irc.org/research/child-rights-in-the-digital-age/92> <http://globalkidsonline.net/about/members/>

92 <http://globalkidsonline.net/about/members/>

5.4.2 POLICY AREA: LEGAL AND REGULATORY

The Year 1 activities listed in the implementation plan under this policy area focus on improving COP knowledge of all law enforcement workers (specifically online harms and investigative techniques) and improvement of formal procedure (including amendments to relevant legislation, introduction of data protection regulations, identification of existing international treaties and protocols, and introducing reporting mechanisms).

CAPACITY BUILDING & TRAINING MATERIALS

Police Scotland delivered a 5-day workshop on COP, 5 representatives from the Government of Rwanda were in attendance, organised by Baroness Kidron. Included in Appendix D are the details of this workshop kindly shared by Superintendent John Wyllie.

Law Enforcement Materials

- ICMEC provides Law Enforcement Training⁹³, and the technology to combat sexual abuse and exploitation
- Such Tools for Law Enforcement⁹⁴ include:
 - PhotoDNA⁹⁵ – Microsoft
 - PhotoDNA: For Industry⁹⁶
 - PhotoDNA: FAQ⁹⁷
 - F1 – Friend MTS⁹⁸ (Media Technology Systems)
 - About⁹⁹ F1 – Friend MTS
 - Griffeye Analyze DI¹⁰⁰ – Safer Society Group
 - About¹⁰¹ Griffeye Analyze DI
- Divisions of the National Crime Agency; Child Sexual Exploitation and Abuse¹⁰² (CEOP), Cybercrime¹⁰³, and National Cyber Crime Unit¹⁰⁴ provide resources

93 <https://www.icmec.org/train/law-enforcement/>

94 <https://www.icmec.org/train/law-enforcement/technology-tools/>

95 <https://www.microsoft.com/en-us/photodna>

96 <https://www.microsoft.com/en-us/PhotoDNA/CloudService>

97 <https://www.microsoft.com/en-us/PhotoDNA/FAQ>

98 <https://www.friendmts.com/>

99 <https://www.icmec.org/press/new-video-fingerprinting-technology-created-to-remove-child-pornography-online/>

100 <https://www.griffeye.com/the-platform/analyze-di/>

101 <https://www.icmec.org/press/the-international-centre-for-missing-exploited-children-receives-major-donation-to-enhance-their-work-combating-child-abuse-and-exploitation/>

102 <http://www.nationalcrimeagency.gov.uk/crime-threats/child-exploitation>

103 <http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime>

104 <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit>

105 <https://virtualglobaltaskforce.com/>

106 <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation>

107 <https://www.interpol.int/>

108 <https://www.interpol.int/Crimes/Crimes-against-children>

109 <https://www.interpol.int/Crimes/Cybercrime>

110 <https://www.interpol.int/Crimes/Human-trafficking>

111 <https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/online-and-on-the-edge.pdf>

112 <https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/in-harms-way.pdf>

113 <https://static1.squarespace.com/static/5a4d5d4e7131a5845cdd690c/1/5c17cdf4032be42f613e28e4/1545063925977/Child+safety+Report+vD+for+web.pdf>

International law enforcement networks

- Virtual Global Taskforce¹⁰⁵ is network dedicated to combatting child sexual abuse
- Europol Cybercrime Centre¹⁰⁶ (EC3) particularly the work of the TWINS Unit on CSE
- INTERPOL¹⁰⁷
 - Crimes Against Children¹⁰⁸
 - Cybercrime¹⁰⁹
 - Human Trafficking¹¹⁰

Reports/ Resources

- Police & Child Online Sexual Exploitation: Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) 2015 Report¹¹¹ "Online and on the edge: Real risks in a virtual world"
- Police & Safeguarding Children: Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) 2015 Report¹¹² "In harm's way: The role of the police in keeping children safe"
- Child Dignity Alliance Technical Working Group Report¹¹³, 2018

See APPENDIX D: REPORT ON GOVERNMENT OF RWANDA VISIT TO POLICE SCOTLAND

REVISING THE LEGISLATIVE FRAMEWORK

Family Online Safety Institute's (FOSI), in partnership with UNICEF, Global Resource and Information Directory (GRID) provides a single, factual data source for a wide array of stakeholders. And can provide insight into legislative activity across jurisdictions. FOSIGRID's information on Rwanda can be found here (Rwanda¹¹⁴).

See APPENDIX E: A REVIEW OF ONLINE CHILD PROTECTION LAWS IN RWANDA

DATA PROTECTION REGULATION

The international standard for data protection is GDPR¹¹⁵, alternatives exist but GDPR is considered the most important change in data privacy regulation in 20 years. See ICO's publication on Children and the GDPR guidance¹¹⁶ and Age Appropriate Design Code, Consultation Document¹¹⁷, published April 2019, to become UK Law.

In Rwanda, data protection currently sits with RURA and data protection regulations are sparse.

See APPENDIX F: DATA PROTECTION REGULATION RECOMMENDATION

RECORDING CRIME

The following is a list of resources, relevant to the recording of crime:

- Home Office Counting Rules For Recorded Crime (including National Crime Recording Standard) April 2018¹¹⁸
- Ministry of Justice Code of Practice for Victims of Crime October 2015¹¹⁹
- Office for National Statistics: Improving Crime Statistics for England and Wales – progress update October 2018¹²⁰
- Resources:
 - Police & Crime-recording: Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) 2014 Report¹²¹ "Crime-recording: making the victim count"

INTERNATIONAL PROTOCOLS

The following is a list of identified international protocols:

- ICMEC: 2018 Model Legislation & Global Review¹²²
- Child Dignity Alliance: 2017 Strategic Plan¹²³
- WeProtect: Model National Response (2016 Guidance¹²⁴)
 - WePROTECT: Global Threat Assessment 2018¹²⁵
 - WePROTECT: Strategy to End Online CSE¹²⁶
- African Union Convention on Cybersecurity and Data Protection¹²⁷

114 <https://fosigrd.org/rwanda>

115 <https://eugdpr.org/>

116 <https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf>

117 <https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf>

118 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/756997/count-general-nov-2018.pdf

119 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/476900/code-of-practice-for-victims-of-crime.PDF

120 <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/methodologies/improvingcrimestatisticsforenglandandwalesprogressupdate>

121 <https://www.justiceinspectores.gov.uk/hmicfrs/wp-content/uploads/crime-recording-making-the-victim-count.pdf>

122 <https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf>

123 <https://static1.squarespace.com/static/5a4d5d4e7131a5845cdd690c/t/5c3608d2032be43c62c8e732/1547045074767/Child%2B Dignity%2B Alliance.Strategic%2BPlan+%286%29.pdf>

124 <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1549388168335/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf>

125 https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5a85ad3253450a61af6b8830/1518710067541/6.4159_WeProtect+GA+report+%281%29.pdf

126 <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/578408b5f7e0ab851b789e14/1479254482761/WePROTECT+Global+Alliance+Strategy.pdf>

127 <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

5.4.3 COP RESPONSE SYSTEMS

The Year 1 activities listed in the implementation plan under this policy area focus on establishing a baseline on removal of CSAM and beginning to implement systems for the removal of CSAM, providing training on offender management to the law enforcement sector, implementing systems for reporting and providing victim support (including providing training to those providing victim support). Rwanda National Police have already established two toll free hotlines, 116 (Child Help Line) and 3512 (GBV reporting line), although effectiveness and awareness of these hotlines would need to be assessed.

REPORTING AND REMOVAL

The following is a list of systems for reporting and removal of illegal online material

Reporting

- Establish an INHOPE Hotlines
 - INHOPE : International Association of Internet Hotlines¹²⁸
 - INHOPE : 2017 Report¹²⁹
 - INHOPE : Guide to setting up Internet Hotline¹³⁰
- The goal of Child Helpline International (CHI) is to improve child protection systems by strengthening child helplines
 - CHI : 2017 Annual Report¹³¹
 - CHI : Toolkits/Manuals¹³²
 - CHI : 2016 Global Data¹³³
 - CHI : Publications¹³⁴
- National Centre for Missing and Exploited Children (NCMEC) International CyberTipline¹³⁵
- #ReplyForAll¹³⁶ acts as a resource for children, concerning internet safety, and allowing children to share their experiences

Removal

Internet Watch Foundation's (IWF) vision is to eliminate child sexual abuse content hosted online, as a direct result, child sexual abuse content hosted in the UK has reduced from 18% in 1996 to below 1% today and content hosted in the UK is removed quickly – usually in less than 2 hours. It is suggested that Rwanda set up a reporting portal with the IWF (information here¹³⁷).

- IWF : 2017 Annual Report¹³⁸
 - Compared to 2005 (first year) Annual Report¹³⁹
- IWF : How to assess and remove content¹⁴⁰

Groupe Spéciale Mobile Association (GSMA) UNICEF provide guidance in this manual: Notice and Takedown: Company policies and practices to remove online child sexual abuse material¹⁴¹

- GSMA: Mobile Alliance Against CSA Content¹⁴²
- GSMA: mYouth¹⁴³

Offender Management

Offender management in the community aims to protect children by reducing risk of further offending both during and post sentence. Listed below are the examples of international best practice:

128 <http://www.inhope.org/gns/home.aspx>

129 http://www.inhope.org/Libraries/Annual_reports/INHOPE_Annual_Report_2017.sflb.ashx

130 https://www.unicef.org/csr/files/GSMA_Inhopebrochure2016_Web.pdf

131 <https://www.childhelplineinternational.org/wp-content/uploads/2018/07/Annual-Report-2017-FINAL.pdf>

132 <https://www.childhelplineinternational.org/child-helplines/tools/>

133 <https://www.childhelplineinternational.org/wp-content/uploads/2017/11/WeListen.pdf>

134 <https://www.childhelplineinternational.org/data-overview/publications/>

135 <http://www.missingkids.org/gethelpnow/cybertipline>

136 <http://replyforall.tumblr.com/>

137 <https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content/our-international-reporting-portals>

138 https://annualreport.iwf.org.uk/pdf/IWF_2017_Annual_Report.pdf

139 https://www.iwf.org.uk/sites/default/files/reports/2016-02/2005_Annual_Report.pdf

140 <https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content>

141 https://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/notice_and_takedown_gsma_unicef_april_2016.pdf

142 <https://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/mobile-alliance>

143 <https://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/myouth>

- Multi-agency public protection arrangements¹⁴⁴ (MAPPA)
 - MAPPA Guidance¹⁴⁵
- Risk Management Authority¹⁴⁶ (RMA) & Risk Assessment Tools Evaluation Directory¹⁴⁷ (RATED)
 - RMA 2017 Corporate Plan¹⁴⁸

Victim Support

To adequately provide support to child victims, all professionals who work with children (e.g. school staff, social workers, health workers, law enforcement workers, lawyers/advocates) must be trained in child protection responsibilities and child safeguarding procedures. Once a crime has been reported to the relevant authorities, multiple agencies should devise measures to be taken to ensure the child is no longer exposed to harm and supported with counselling, that best mitigates any long-term psychological impact of abuse.

VICTIM SUPPORT: SAFEGUARDING

- Safeguarding: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children 2018 Report¹⁴⁹
 - Complimentary guidance from (National Institute for Health and Care Excellence) NICE:
 - Child Abuse and Neglect¹⁵⁰
 - Harmful sexual behaviour among children and young people¹⁵¹
- General Medical Council: Ethical Guidance for doctors, Guidance on treating children and young people¹⁵²
- Royal College of Paediatrics and Child Health, Safeguarding children and young people: roles and competences for health care staff March 2014¹⁵³
- British Psychological Society Safeguarding Children and Young People: Every Psychologist's Responsibility¹⁵⁴

- 144 <https://www.gov.uk/government/publications/multi-agency-public-protection-arrangements-mappa--2>
- 145 <https://mappa.justice.gov.uk/connect/ti/MAPPA/view?objectId=271411&exp=e2>
- 146 <https://www.rma.scot/>
- 147 <http://rated.rmascotland.gov.uk/>
- 148 https://www.rma.scot/wp-content/uploads/2018/03/Corp_Plan_2017_web.pdf
- 149 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779401/Working_Together_to_Safeguard_Children.pdf
- 150 <https://www.nice.org.uk/guidance/ng76/chapter/About-this-guideline>
- 151 <https://www.nice.org.uk/guidance/ng55>
- 152 <https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors#children-young-people>
- 153 https://www.rcpch.ac.uk/sites/default/files/Safeguarding_children_Roles_and_Compences_for_Healthcare_Staff_Third_Edition_March_2014.pdf
- 154 <https://www.bps.org.uk/news-and-policy/safeguarding-children-and-young-people-every-psychologists-responsibility>
- 155 https://www.minded.org.uk/Catalogue/Index?HierarchyId=O_39474_39502&programmId=39474
- 156 <https://youngminds.org.uk/media/1520/youngminds-sexual-abuse.pdf>
- 157 <https://youngminds.org.uk/find-help/for-parents/parents-guide-to-support-a-z/parents-guide-to-support-abuse/>
- 158 https://www.childrensociety.org.uk/what-is-child-sexual-exploitation?gclid=Cj0KCQIAN4PkBRCDARIsAGHmH3fz-DR34rUj1JEiGt_5C6YRgdez4BIFnAQPU4vQVFa45T-LWuJt4QaAtBBEALw_wcB
- 159 <https://www.childrensociety.org.uk/knowing-the-signs-of-child-sexual-exploitation>
- 160 <https://www.nice.org.uk/guidance/ng76/chapter/Recommendations#therapeutic-interventions-for-children-young-people-and-families-after-child-abuse-and-neglect>
- 161 <https://learning.nspcc.org.uk/services-children-families/letting-the-future-in/#article-top>

VICTIM SUPPORT: INFORMATION FOR COUNSELLORS/ THERAPISTS/ PSYCHOLOGISTS

- UK Royal Colleges (MindEd) provides a catalogue of information¹⁵⁵ in relation to wellbeing
- Young Minds provides guidance for sexual abuse victims¹⁵⁶, and to guidance to parents¹⁵⁷ who believe their child may have been a victim of sexual abuse
- The Children's Society provides information on child sexual exploitation¹⁵⁸ and how to recognise the signs¹⁵⁹

VICTIM SUPPORT: COUNSELLING

- NICE guidance on Therapeutic interventions for children, young people and families after child abuse and neglect¹⁶⁰
- Young People who are/have been victims of Sexual Abuse:
 - **Letting the Future In**¹⁶¹
NICE guidelines refer to 'Letting the Future In' as an intervention for children and young people (boys or girls) aged 8 to 17 who have been sexually abused and is considered as best practice in such cases. The programme; (1) emphasises the importance of the therapeutic relationship between the child or young person and therapist, (2) offers support tailored to the child or young person's needs, drawing on a range of approaches including counselling, socio-educative and

creative (such as drama or art) and (3) includes individual work with the child or young person (up to 20 sessions, extending to 30 as needed) and parallel work with non-abusing parents or carers (up to 8 sessions).

- **Protect and Respect**¹⁶²

Protect and Respect is a prevention programme, in the process of being evaluated by University of Bedfordshire. It is currently in line with best practice but will improve as the evaluation informs quality improvements.

- **Hear and Now**¹⁶³

This programme has not been fully evaluated but is derived from 'Letting the Future In', so should be in line with best practice.

Another therapeutic intervention would be for parents to provide support, but parents would need to be supported to do so. If guidance were to be created, a joint collaboration between schools, parents and counsellors would be the ideal scenario in which to create a protocol

¹⁶² <https://learning.nspcc.org.uk/services-children-families/protect-and-respect/>

¹⁶³ <https://learning.nspcc.org.uk/services-children-families/hear-and-now/>

The Year 1 activities listed in the implementation plan under this policy area focus on holding industry round tables to discuss corporate responsibility, protections from commercial pressures, implementation of safety/security features by design and default.

To support these discussions, the research team have provided a list of resources including corporate responsibility (Safety-by-design standards), protections from commercial pressures, and safety software (including age verification). These are all fast-moving areas and will require constant updating.

CORPORATE RESPONSIBILITY

- UNCRC General Comment on Children’s rights in relation to the digital environment¹⁶⁴
- UNICEF & Better Business for Children¹⁶⁵
 - UNICEF & Better Business for Children: Children’s Rights & Internet¹⁶⁶
 - UNICEF & Better Business for Children: Tools for ICT companies¹⁶⁷
 - UNICEF & Better Business for Children: Good Practice Examples¹⁶⁸
- ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights¹⁶⁹
- ITU
 - ITU Guidelines for Industry on COP 2014 Edition¹⁷⁰
 - Case Studies (including mobile providers¹⁷¹, internet services providers¹⁷², content providers¹⁷³, user generated content¹⁷⁴, broadcasters¹⁷⁵ and manufacturers¹⁷⁶)
- Lessons on COP for industry, published by UNICEF
 - Children’s Rights in ICT Sector (Module 1 PDF¹⁷⁷)
 - Child Online Protection Guidelines for the ICT Sector (Module 2 PDF¹⁷⁸)
 - Carrying Out Child Rights Due Diligence in the ICT Sector (Module 3 PDF¹⁷⁹)
 - Child Right’s Due Diligence for Mobile Operators (Module 4 PDF¹⁸⁰)
 - Child Rights Due Diligence for Online and Mobile Games and Application Development (Module 5 PDF¹⁸¹)

164 <https://5rightsfoundation.com/in-action/uncrc-general-comment-on-childrens-rights-in-relation-to-the-digital-environment.html>

165 <https://www.unicef.org/csr/>

166 <https://www.unicef.org/csr/childrensrighsandinternet.htm>

167 <https://www.unicef.org/csr/toolsforcompanies.htm>

168 <https://www.unicef.org/csr/goodpractices.htm>

169 <https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide ICT.pdf>

170 https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf

171 <https://www.itu.int/en/cop/case-studies/Pages/sector1.aspx>

172 <https://www.itu.int/en/cop/case-studies/Pages/sector2.aspx>

173 <https://www.itu.int/en/cop/case-studies/Pages/sector3.aspx>

174 <https://www.itu.int/en/cop/case-studies/Pages/sector4.aspx>

175 <https://www.itu.int/en/cop/case-studies/Pages/sector5.aspx>

176 <https://www.itu.int/en/cop/case-studies/Pages/sector6.aspx>

177 https://www.unicef.org/csr/files/Training_Module_1_Child_Rights_and_the ICT_Sector.pdf

178 https://www.unicef.org/csr/files/Training_Module_2_Child_Online_Protection_for ICT_industry.pdf

179 https://www.unicef.org/csr/files/Training_Module_3_Carrying_out_Child_Rights_Due_diligence_for_the ICT_Sector.pdf

180 https://www.unicef.org/csr/files/Training_Module_4_Child_Rights_Due_diligence_for_Mobile_Operators.pdf

181 https://www.unicef.org/csr/files/Training_Module_5_COSA_for_Online_Games_and_Apps.pdf

182 <https://d1qmdf3vop2l07.cloudfront.net/eggplant-cherry.cloudvent.net/compressed/c1c90b5e630cd6bac92b6ad41afab22d.pdf>

183 <https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf>

184 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/487973/ukccis_guide- final_3_.pdf

185 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

186 <https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm>

187 <https://www.esafety.gov.au/esafety-information/safety-by-design>

SAFETY-BY-DESIGN STANDARDS

- 5 Rights Towards an Internet Safety Strategy¹⁸² 2019
- 5Rights Foundation’s Report “Disrupted Childhood: The Cost of Persuasive Design”¹⁸³
- UKCCIS: A Practical Guide for Providers of Social Media and Interactive Services¹⁸⁴
- UK government, Internet Safety Strategy¹⁸⁵ Green Paper 2017
- House of Lords Select Committee on Communications Growing up with the internet¹⁸⁶
- Australian Government eSafety Commissioner Safety by Design¹⁸⁷

PROTECTION FROM COMMERCIAL PRESSURES

- House of commons Briefing Paper October 2018: Advertising to children¹⁸⁸
- Advertising Standards Agency (ASA) New guidance launched for social influencers¹⁸⁹
- Norwegian Consumer Council (Forbrukerrådet) Deceived by Design¹⁹⁰

SAFETY SOFTWARE/DEFAULT CHILD APPROPRIATE FILTERS

- Contact WeProtect Global Alliance for Registry of Technical Solutions¹⁹¹
- Identity
 - Gov.uk Verify¹⁹²
- Resources for Parents:
 - NSPCC Guidance Parental Controls: Webpage¹⁹³
 - UK Safer Internet Centre: Parental Controls¹⁹⁴
- Resources for Schools:
 - UK Safer Internet Centre: Filtering and Monitoring in Schools¹⁹⁵
 - NEN Education Network: Advice for Schools¹⁹⁶
 - Online Safety self-review tool for schools: 360 degree safe Webpage¹⁹⁷
 - Keeping children safe in education Statutory guidance for schools and colleges (Annex C Online Safety¹⁹⁸ – pg. 93)

AGE VERIFICATION

- British Board of Film Classification (BBFC) Age Verification Regulator¹⁹⁹

188 <http://researchbriefings.files.parliament.uk/documents/CBP-8198/CBP-8198.pdf>

189 <https://www.asa.org.uk/news/new-guidance-launched-for-social-influencers.html>

190 <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>

191 weprotect.org

192 <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>

193 <https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/parental-controls/>

194 <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/parental-controls-offered-your-home-internet-provider>

195 <https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring>

196 <http://www.nen.gov.uk/advice>

197 <https://360safe.org.uk/>

198 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741314/Keeping_Children_Safe_in_Education_3_September_2018_14.09.18.pdf

199 <https://www.ageverificationregulator.com/>

5.4.5 EDUCATION

The Year 1 activities listed in the implementation plan under this policy focus on implementing child protection and safeguarding procedures in schools (with provisions for COP related issues), delivering COP training to all teachers and school staff, implementing COP sessions in lessons in Rwandan schools and at The University of Rwanda as part of their citizenship module, and generally promoting positive internet use. .

GUIDANCE TO SCHOOLS ON COP

Child protection and safeguarding policies in school are a crucial element of keeping safe. The PIES model²⁰⁰ is a useful guide to follow and is a long-established approach to whole school online safety.

Policy – these will provide clarity and consistency of approach. Everyone has the same understanding and schools can work to a set of minimum requirements. It is important to be clear about what schools must do and what schools should do. The terms “must” and “should” are used throughout: “must” when the organisation or individual in question is required to do something and “should” when the advice set out should be followed unless there is good reason not to.

Infrastructure – consideration should be given to the technical solutions which schools can provide to keep children safe online (e.g. filtering and monitoring). Whilst important, this cannot be done in isolation, blocking, restricting and banning does not work as evidenced by this recent research²⁰¹ – education (see below) is the most important (and effective) aspect of a whole-school online safety approach

Education – Dialogue, discussion and positive communication is a vital element of effective COP. An education programme should provide opportunities for children and young people to talk about what they are doing online, to celebrate the opportunities and benefits as well as discuss and consider the potential risks and challenges.

Education for parents, carers and teachers is also important and this needs to be ongoing. In a rapidly changing world it is important that adults who are working with children and young people are equipped with the knowledge and understanding to have meaningful dialogue about the risks and opportunities. Good quality CPD needs to take place and be updated on a regular basis.

Standards/Impact/Effectiveness – assessing the effectiveness of online safety programmes is an ongoing challenge. Children and young people may seem to be aware of online safety issues but the extent to which this awareness is reflected in their online behaviour is another matter entirely.

200 <https://www.jisc.ac.uk/guides/internet-safety>

201 <https://www.sciencedaily.com/releases/2018/04/180403144447.htm>

Continuing professional development

- Better Internet for Kids Bulletin²⁰² – a quarterly publication with up to date information, news and resources on the latest trends in online life.

Possible accreditation for schools

- Esafety Label²⁰³ – an accreditation and support service for schools, aiming to provide a secure and enriching environment, for safe access to online technology as part of the teaching and learning experience.
- 360 safe²⁰⁴ – a free online safety self-review tool for schools

202 <https://us6.list-manage.com/subscribe?u=fcaa73d53911340a72d92d73f&id=ca4e66ba46>

203 <https://www.esafetylabel.eu/home>

204 <https://360safe.org.uk/>

205 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779401/Working_Together_to_Safeguard_Children.pdf

206 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/722307/Working_Together_to_Safeguard_Children_Statutory_framework.pdf

207 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741314/Keeping_Children_Safe_in_Education__3_September_2018_14.09.18.pdf

208 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/562876/Guidance_for_School_Governors_-_Question_list.pdf

209 <https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/#article-top>

210 <https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring>

211 <https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring>

212 <https://reportharmfulcontent.com/>

213 <https://www.gov.uk/government/publications/searching-screening-and-confiscation>

214 <https://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety>

215 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781150/Draft_guidance_Relationships_Education_Relationships_and_Sex_Education_RSE_and_Health_Education2.pdf

216 <https://www.itu.int/en/cop/Documents/S-GEN-COP.EDUC-2016-PDF-E%5b1%5d.pdf>

217 <https://swgfl.org.uk/>

218 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/683895/Education_for_a_connected_world_PDF.pdf

219 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_g_In_Schools_FINAL_Update_Jan17.pdf

220 <https://www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges>

221 <https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring>

222 <http://www.nen.gov.uk/advice>

223 <https://360safe.org.uk/>

224 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741314/Keeping_Children_Safe_in_Education__3_September_2018_14.09.18.pdf

COP RESOURCES FOR SCHOOLS

School Safeguarding

- Safeguarding: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children 2018 Report²⁰⁵
 - Working Together to Safeguard Children Statutory framework: legislation relevant to safeguarding and promoting the welfare of children July 2018²⁰⁶
- UK Department of Education Keeping children safe in education Statutory guidance for schools and colleges 2018 Report²⁰⁷

School COP Policies

- UKCCIS Online safety in schools and colleges: Questions from the Governing Board²⁰⁸
- NSPCC E-Safety for Schools Webpage²⁰⁹
- UK Safer Internet Centre Guidance for Teachers and School Staff²¹⁰
 - Professionals Online Safety Helpline²¹¹
- Reporting Harmful Content Hub²¹²
- Searching, screening and confiscation at school Guidance²¹³
- Kelsi: Online safety policies²¹⁴
- UK Gov, Department for Education: Relationships and Sex Education²¹⁵ – new guidance from which includes online safety

COP Resources for Educators

- ITU Guidelines for Parents, Guardians and Educators on Child Online Protection 2016²¹⁶
- South West Grid for Learning (SWGfL) Template for setting out online safety policies²¹⁷
- UKCCIS: Education for a Connected World²¹⁸
- UKCCIS: Sexting in schools and colleges²¹⁹
- UK Gov : Sexual violence and sexual harassment between children in schools and colleges²²⁰
- Information on Filtering/Safety Resources for Schools:
 - UK Safer Internet Centre: Filtering and Monitoring in Schools²²¹
 - NEN Education Network: Advice for Schools²²²
 - Online Safety self-review tool for schools: 360 degree safe Webpage²²³
 - Keeping children safe in education Statutory guidance for schools and colleges (Annex C Online Safety²²⁴ – pg. 93)

Lessons in Schools

- Child Exploitation and Online Protection Command (CEOP) Thinkuknow Education Programme²²⁵
- Ten principles of effective PSHE education²²⁶
- POLICE IN THE CLASSROOM A handbook for the police and PSHE teachers²²⁷
- Specific messages:
 - Online safety/pornography Guidance from Personal, Social, Health and Economic (PSHE)²²⁸
 - Relationships/Sexting disrespectnobody²²⁹
 - Cyberbullying Guidance²³⁰
 - Extremism/radicalisation educateagainsthate²³¹
- NSPCC Preventing Abuse:
 - Online abuse²³²
 - Grooming²³³
 - Child Sexual Exploitation²³⁴
 - Sexual Abuse²³⁵
 - Bullying/Cyberbullying²³⁶
- The ENABLE Project provides Guidance on Cyberbullying²³⁷
- United Kingdom Chief Medical Officers' commentary²³⁸ on "Screen-based activities and children and young people's mental health and psychosocial wellbeing"

225 <https://www.thinkuknow.co.uk/>

226 <https://www.pshe-association.org.uk/curriculum-and-resources/resources/ten-principles-effective-pshe-education>

227 https://www.pshe-association.org.uk/sites/default/files/u26918/CYP_police_in_the_classroom_handbook.pdf

228 <https://www.pshe-association.org.uk/>

229 <https://www.disrespectnobody.com/relationship-abuse/what-is-relationship-abuse/>

230 <https://www.childnet.com/resources/cyberbullying-guidance-for-schools>

231 <https://educateagainsthate.com/>

232 <https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/keeping-children-safe/>

233 <https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/grooming/>

234 <https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/child-sexual-exploitation/preventing-cse/>

235 <https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/child-sexual-abuse/helping-children/>

236 <https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/bullying-and-cyberbullying/>

237 http://enable.eun.org/implementing_enable

238 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777026/UK_CMO_commentary_on_n_screentime_and_social_media_map_of_reviews.pdf

239 <https://5rightsfoundation.com/>

240 https://5rightsfoundation.com/static/Digital_Childhood_report_-_EMBARGOED.pdf

241 <https://digital-literacy.org.uk/>

242 <https://www.saferinternet.org.uk/pupil-powered-e-safety>

243 <https://digital-leaders.childnet.com/>

244 <https://www.childnet.com/resources/film-competition/2016>

245 <https://community.computingschool.org.uk/resources/43/single>

246 <https://www.cyberfirst.ncsc.gov.uk/girlscompetition/>

247 <http://humanetech.com/take-control/>

248 <https://www.common sense.org/education/>

Promoting Digital Literacy

- 5Rights Data Literacy for Kids Programme²³⁹
- 5Rights Digital Childhood Report DIGITAL CHILDHOOD Addressing Childhood Development Milestones in the Digital Environment²⁴⁰
- South West Grid for Learning (SWGfL) Digital Literacy and Citizenship materials²⁴¹
- UK Safer Internet Centre Pupil-Powered E-Safety²⁴²
- Childnet Digital Leaders²⁴³, Film Competition²⁴⁴
- Student challenges (e.g. UK challenges²⁴⁵)
- Cyber First Girls Competition²⁴⁶

Promoting Healthy Internet Habits

- Centre for Humane Technology's guidance to "Take control of your phone²⁴⁷"
- Common Sense Media's guides on internet use for educators and students²⁴⁸

5.4.6 PUBLIC AWARENESS OF COP

The Year 1 activities listed in the implementation plan under this policy focus on educating the public (by creating and disseminating messages about COP and establishing a government webpage for public information) and to educate parents (to increase parents' awareness of COP and implement interventions in the home environment).

PUBLIC AWARENESS STRATEGY

Messaging is key to ensuring immediate intervention. School staff and professionals engaging with children have little awareness of COP (due to lack of exposure to technology, lack of exposure to online harms, and lack of education on online safety), but acknowledge that cases of online harms are beginning to emerge. Therefore, interventions need to be made immediately in the home, by educating children and parents on COP

TRAINING FOR PARENTS AND YOUNG CHILDREN

Below is a list of potential COP resources for parents and children, COP education in the home is an emerging area and requires greater development. Listed below are examples of what is currently available:

- Children:
 - ITU Guidelines for Children on Child Online Protection²⁴⁹
 - CEOP Thinkuknow Programme²⁵⁰
 - Childnet resources²⁵¹
- Parents:
 - ITU Guidelines for Parents, Guardians and Educators on Child Online Protection 2016²⁵²
 - UKCIS Child Safety Online: A practical guide for parents and carers whose children are using social media²⁵³
 - Get Safe Online, Safeguarding for Parents²⁵⁴
 - Risk rating of specific apps/services Net Aware²⁵⁵
 - CEOP ThinkuKnow Programme²⁵⁶
 - Childnet resources²⁵⁷
 - Internet safety (see above – school/education programmes)

249 <https://www.itu.int/en/cop/Documents/S-GEN-COP.CHILD-2016-PDF-E%5b1%5d.pdf>

250 <https://www.thinkuknow.co.uk/>

251 <https://www.childnet.com/>

252 <https://www.itu.int/en/cop/Documents/S-GEN-COP.EDUC-2016-PDF-E%5b1%5d.pdf>

253 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Guidance_UKCCIS_Final_18122015.pdf

254 <https://www.getsafeonline.org/safeguarding-children/>

255 <https://www.net-aware.org.uk/networks/?order=title>

256 <https://www.thinkuknow.co.uk/>

257 <https://www.childnet.com/>

There is currently little published research on COP in Rwanda. Therefore, Year 1 activities listed in the implementation plan under this policy focus upon key issues including, the development of a research community on COP in Rwanda, by establishing research priorities, collecting baseline data, training the innovation community on COP and identifying leadership in this area.

For the purposes of supporting these activities, the research team have provided a list of potential research priorities, examples of international COP research groups, international centers of excellence on COP (and other related fields), and examples of COP (or related) conferences. It is recommended that when creating a research group, those involved should aim to create research that uses both rigorous quantitative and qualitative methods, those affected should be central to the research programme and relevant expert stakeholders should be utilized to influence the direction of new research projects or to partner on research projects.

AREAS OF POTENTIAL RESEARCH

- internet penetration, internet use, use of devices, online experiences of children of different age ranges;
- children’s experience and understanding of online risk and safety using international terminology
- needs assessments, identifying prevalence, trends in different areas of risk and harm
- e-health interventions to address mental health, violence and abuse;
- regulatory interventions to foster corporate responsibility and safety by design;
- victim support counselling;
- monitoring, identifying compliance with policy and implementation of interventions to promote child online safety;
- prototyping and evaluating COP training and messaging strategies
- effectiveness, evaluating the costs and impacts of specific interventions to identify best buys and establish impact.

EXAMPLES OF RELEVANT RESEARCH GROUPS/PROGRAMMES

- UKCIS Evidence Group²⁵⁸ (Chaired by Prof Julia Davidson) (webpage²⁵⁹)
 - Children’s online activities, risks and safety: A literature review by the UKCCIS Evidence Group 2017 Report²⁶⁰
 - Research Highlight Series²⁶¹
- UNICEF Innocenti Research Centre²⁶²
- Innocenti Research Centre: Researching Children’s Rights Globally in the Digital Age²⁶³
- Global Kids Online²⁶⁴ (Prof Sonia Livingstone)
 - Global Kids Online: Tools for Researchers²⁶⁵
 - Global Kids Online: Research Results²⁶⁶
- Digitally Connected²⁶⁷
- Independent Inquiry into child sexual abuse research programme (IICSA)²⁶⁸
- Relevant research funded by the EC and End Violence Against Children
 - End Violence Against Children Grantees²⁶⁹

258 <https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis#working-groups>

259 <https://www.saferinternet.org.uk/research>

260 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf

261 <https://www.saferinternet.org.uk/research/research-highlight-series>

262 <https://www.unicef-irc.org/>

263 <https://www.unicef-irc.org/knowledge-pages/Researching-Children-s-Rights-Globally-in-the-Digital-Age/>

264 <http://globalkidsonline.net/>

265 <http://globalkidsonline.net/tools/>

266 <http://globalkidsonline.net/results/>

267 <http://www.digitallyconnected.org/>

268 <https://www.iicsa.org.uk/>

269 <http://www.end-violence.org/fund/grantees>

CENTRES OF EXCELLENCE

Establishing University of Rwanda as a centre of excellence will be facilitated by development of a long-term partnership with well-established centres of excellence in the global north with a focus on capacity development and enabling local leadership. For example:

- Centre for Excellence for Looked After Children in Scotland (CELCIS)²⁷⁰
- The International Centre for Child Protection (Kent University)²⁷¹
- Social care institute for excellence (SCIE)²⁷²
- University of Bedfordshire, Professor Jenny Pearce²⁷³
 - The International Centre: Researching child sexual exploitation, violence and trafficking²⁷⁴
- Centre for abuse and Trauma Studies²⁷⁵ (CATS) (see Prof Julia Davidsons' research²⁷⁶)

COP CONFERENCES

- NSPCC 'How Safe Are Our Children?' Growing up online 2.0 June 2019²⁷⁷
 - Conference Agenda²⁷⁸
- World Internet Conference²⁷⁹, Cyberspace Administration of China
- ITU's Regional Conference on Africa Child Online Protection (ACOP)²⁸⁰: Empowering the Future Digital Citizens
- Internet Governance Forum²⁸¹
- Dynamic Coalition on Child Online Safety²⁸²

270 <https://www.celcis.org/>

271 <https://www.kent.ac.uk/sspsr/ccp/>

272 <https://www.scie.org.uk/children/>

273 <https://www.beds.ac.uk/news/experts/jenny-pearce>

274 <https://www.beds.ac.uk/ic>

275 <https://catsresearch.org.uk/>

276 <https://catsresearch.org.uk/publications/>

277 <https://learning.nspcc.org.uk/news/2019/june/how-safe-are-our-children-conference-2019/>

278 <https://learning.nspcc.org.uk/media/1633/how-safe-are-our-children-agenda-2019.pdf>

279 <http://www.wuzhenwic.org/>

280 <https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Pages/EVENTS/ACOP2013/default.aspx>

281 <https://www.intgovforum.org/multilingual/>

282 <http://www.intgovforum.org/cms/dynamic-coalitions-49674/79-child-online-safety#introduction>

Appendix

| | |
|--|----|
| A. COP ORGANISATIONS | 72 |
| B. COP MODULE OUTLINE FOR TEACHERS AND EDUCATORS | 74 |
| C. TERMINOLOGY GUIDELINES FOR COP | 76 |
| D. REPORT ON GOVERNMENT OF RWANDA VISIT TO POLICE SCOTLAND | 89 |
| E. A REVIEW OF ONLINE CHILD PROTECTION LAWS IN RWANDA | 93 |
| F. DATA PROTECTION REGULATION RECOMMENDATION | 96 |
| G. FURTHER READING ON THE RWANDAN CONTEXT | 98 |

APPENDIX A: COP ORGANISATIONS

| Acronym | Organisation Name | Home Page Link |
|-----------------|---|---|
| | 5Rights Foundation | https://5rightsfoundation.com/ |
| ASA | Advertising Standards Agency | https://www.asa.org.uk/ |
| BBFC | British Board of Film Classification | https://www.bbfc.co.uk/ |
| CQC | Care Quality Commission | https://www.cqc.org.uk/ |
| | Centre for Humane Technology | http://humanetech.com/ |
| CJCP | Centre for Justice and Crime Prevention | http://www.cjcp.org.za/ |
| | Child Dignity Alliance | https://www.childdignity.com/child-dignity-alliance |
| CEOP | Child Exploitation and Online Protection Centre | https://www.ceop.police.uk/safety-centre/ |
| CHI | Child Helpline International | https://www.childhelplineinternational.org/ |
| | Child Rights Connect | https://www.childrightsconnect.org/ |
| | Childnet | https://www.childnet.com/ |
| | Common Sense Media | https://www.common sense media.org/ |
| | Commonwealth Cybercrime Initiative | http://thecommonwealth.org/commonwealth-cybercrime-initiative |
| CT | Commonwealth Telecommunications Organisation | https://cto.int/ |
| | Digitally Connected | http://www.digitallyconnected.org/ |
| EVAC | End Violence Against Children | http://www.end-violence.org/ |
| EUROPOL | European Union Agency for Law Enforcement Cooperation | https://www.europol.europa.eu/ |
| ECPAT | Every Child Protected Against Trafficking | https://www.ecpat.org/ |
| FOSI | Family Online Safety Institute | https://www.fosi.org/ |
| | Get Safe Online | https://www.getsafeonline.org/ |
| | Global Kids Online | http://globalkidsonline.net/ |
| GRID | Global Resource and Information Directory | https://fosigrid.org/ |
| GSMA | Groupe Spéciale Mobile Association | https://www.gsma.com/ |
| ICO | Information Commissioners Office | https://ico.org.uk/ |
| | INHOPE Foundation | http://www.inhopefoundation.org/ |
| ICMEC | International Centre for Missing and Exploited Children | https://www.icmec.org/ |
| INTERPOL | International Criminal Police Organization (ICPO) | https://www.interpol.int/ |
| ITU | International Telecommunications Union | https://www.itu.int/ |

| | | |
|-------------------------|---|---|
| IWF | Internet Watch Foundation | https://www.iwf.org.uk/ |
| Kelsi | Kelsi | https://www.kelsi.org.uk/# |
| MAPPA | Multi-agency public protection arrangements | https://www.gov.uk/government/publications/multi-agency-public-protection-arrangements-mappa--2 |
| NCMEC | National Centre for Missing and Exploited Children | http://www.missingkids.com/home |
| NCA | National Crime Agency | https://nationalcrimeagency.gov.uk/ |
| NEN | National Education Network | http://www.nen.gov.uk/ |
| NICE | National Institute for Health and Care Excellence | https://www.nice.org.uk/ |
| NSPCC | National Society for the Prevention of Cruelty to Children | https://www.nspcc.org.uk/ |
| | Net Aware | https://www.net-aware.org.uk/networks/?order=title |
| PSHE Association | Personal, Social, Health and Economic Education Association | https://www.pshe-association.org.uk/ |
| RATED | Risk Assessment Tools Evaluation Directory | http://rated.rmascotland.gov.uk/ |
| RMA | Risk Management Authority | https://www.rma.scot/ |
| | Save the Children | https://www.savethechildren.net/ |
| SWGfL | South West Grid for Learning | https://swgfl.org.uk/ |
| | The ENABLE Project | https://www.theenableproject.co.uk/ |
| UKCCIS | UK Council for Child Internet Safety | https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis |
| UKCIS / UKCCIS | UK Council for Internet Safety / UK Council for Child Internet Safety | https://www.gov.uk/government/organisations/uk-council-for-internet-safety |
| | UK Safer Internet Centre | https://www.saferinternet.org.uk/ |
| | UKCIS Evidence Group | https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis#working-groups |
| UNICEF | UNICEF Innocenti Research Centre | https://www.unicef-irc.org/ |
| | United Nations Children's Fund | https://www.unicef.org/ |
| | Virtual Global Taskforce | https://virtualglobaltaskforce.com/ |
| | WePROTECT | https://www.weprotect.org/ |

APPENDIX B: COP MODULE OUTLINE FOR TEACHERS AND EDUCATORS

PROVIDED BY KARL HOPWOOD

The whole area of online safety is fast moving, and we know that teachers and other professionals often feel ill-equipped to address the challenges.

The International Telecommunications Union (ITU) through their Child Online Protection Initiative²⁸³ noted that in most cases parents and guardians are not aware of details concerning the online experiences their children are likely to encounter and the risks and vulnerabilities related to various online activities. Schools clearly have a key role to play in raising awareness of some of the key risks but also in providing opportunities for children and young people to ask questions about the challenges that they face online. Dialogue and discussion are crucial, and schools need to understand both what children and young people are doing when they are online as well as where the risks and opportunities lie.

Research carried out in 2018²⁸⁴ found that 61% of respondents (head teachers and safeguarding leads in schools) said that they did not receive sufficient guidance from government bodies and local authorities around peer on peer abuse. The report concluded that it is unreasonable to expect school leaders to become experts in all aspects of safeguarding without appropriate support and resources. Training is an essential part of effective online safety education, yet it is an area where there is least focus and resource.

OUTLINE

Ideally online safety training should be a statutory part of initial teacher training as well as continuing professional development. Best practice would suggest that a lot of this content should be embedded within safeguarding training with some aspects being picked up as part of more bespoke sessions. Teachers should be equipped with an understanding of the challenges that children and young people are facing online but also with some proven approaches for addressing these effectively. Much work has been done in recent years and a number of useful resources have been developed. Individual ITT organisations will need to determine how much time can be allocated to issues around online safety and also those areas which need to be covered and in how much detail.

²⁸³ [https://www.itu.int/en/cop/Documents/S-GEN-COP.EDUC-2016-PDF-E\[1\].pdf](https://www.itu.int/en/cop/Documents/S-GEN-COP.EDUC-2016-PDF-E[1].pdf)

²⁸⁴ https://www.mariecollinsfoundation.org.uk/assets/news_entry_featured_image/MCF-Peer-on-peer-Abuse-Research-Report-sunday-final-version.pdf

²⁸⁵ <https://download.microsoft.com/download/4/4/F/44F46E37-D937-42FC-B7E7-16F2EE8COC71/Microsoft-Policymaker-Guide-Online-Safety.pdf>

CONTENT

A sensible approach with regards to the areas of online safety that need to be covered would be to focus on content, contact, conduct and commercial risks. These are often referred to as the 4 Cs and have been widely adopted by many organisations across the world.²⁸⁵

Further work has been done to identify more precisely what children and young people should be taught about online safety. There is also some discussion about the age at which children and young people should be introduced to online safety at school or at home. Ideally this should start as soon as they are using devices that are capable of going online.

The UK Council for Child Internet Safety (UKCCIS) (now renamed as the UK Council for Internet Safety)'s Education Working Group has published a framework Education for a Connected World which aims to map out the skills and competences that children and young people should have across eight different areas of online safety at different ages and stages. The eight areas (listed below) clearly show that online safety should not simply be addressed as part of the technology curriculum but as a whole-school, cross-curricular issue.

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security
- Copyright and ownership

Schools should have their own policies relating to online safety and these should include provision about how staff should be using technology within the classroom and around school. It is important that teachers are aware of these policies within their schools and fully understand them.

DELIVERY

Comprehensive lesson plans are available to teach most aspects of online safety, but the most effective approach will be to tailor and adapt some of these existing resources to suit the needs of particular groups of pupils. As mentioned earlier, identifying opportunities for discussion and dialogue is important in such a fast-moving space. The list below contains some of the issues which should/could be addressed.

Outline of the issues – what are the risks that children and young people are facing when they go

online? The challenge is to determine where the focus should be, and local knowledge is important here.

What considerations do professionals need to have when they are online? Online reputation, cyberbullying, exposure to inappropriate content, malware and viruses, identity theft etc.

The challenges of delivering the subject e.g. lack of parental engagement/understanding, rapid development of technology and new/emerging risks, difficulties with engaging children and young people in meaningful dialogue around the issues, culture of banning, negative press coverage etc.

- Working in partnership with parents, carers and the wider community
- Successful approaches e.g. peer to peer education, digital leaders
- How to provide safe access at school – filtering, monitoring, education – without harming children's rights?
- How to assess the impact of what is being done? Does it work, does it make children and young people safer? Does it increase resilience?
- How to develop a whole school policy? Children and young people (as well as other stakeholders) need to be involved in this.
- Approach
- Discussion of case studies – what would you do?
- Overview of the issues and current/upcoming risks.
- Awareness of available resources – identification of gaps in provision/resource.
- Ability to then localise to suit the needs of the individual school/class.

Multi-agency training for adults can be useful once teachers are in post as a way of keeping them up to date – sharing concerns and experiences with others such as law enforcement officers, social care and health professionals as well as those in education can be powerful and produce a more meaningful dialogue.

IMPACT

It is important to measure the impact that online safety education has on children and young people – it is very easy to be able to recite some rules for staying safe but much more difficult to effect a change in behaviour or to demonstrate increased resilience. Teachers should feel confident that they have the skills and the tools that they need to deliver effective online safety education for their pupils – a particular challenge in a world where the media would have us believe that children and young people know more about technology than adults. A good teacher will be able to facilitate a discussion around the issues without necessarily needing to be an expert. Equally some consideration should be given as to how to evaluate the

effectiveness of the CPD for teachers – is it fit for purpose, is it relevant and up to date. Do they feel empowered to discuss these issues with their pupils?

APPENDIX C: TERMINOLOGY GUIDELINES FOR COP

All terms and guidance have been taken from the Luxembourg Guidelines, see page numbers reference for detailed guidance and use of each term. The use of **red** terms should be avoided. Special attention should be paid to how **orange** terms are used. **Green** terms appear to have a generally agreed meaning and/or can be used without stigmatising and/or otherwise harming the child. **Bold** terms are key terms.

| Term | Definition | Other related terms | Guidance |
|---------------------------------|---|---|-----------|
| Adolescent | The period in human growth and development that occurs after childhood and before adulthood, from ages 10 to 19. | Child, Age of majority, Age of sexual consent, Minor, Juvenile, Teenager, Young person/young people/youth | pp. 9–10 |
| Age of majority | [Legal Term] Age at which a person becomes an adult, with all the attendant rights and responsibilities of adulthood. In many countries, the age of majority is set at 18. | Child, Age of sexual consent, Minor, Juvenile, Adolescent, Teenager, Young person/young people/youth | p. 6 |
| Age of sexual consent | The age below which it is prohibited to engage in sexual activities with a child. The legal age of sexual consent varies between countries, although many set the age of sexual consent at between 14 and 16 years of age. | Child, Age of majority, Minor, Juvenile, Adolescent, Teenager, Young person/young people/youth | pp. 7–8 |
| Child | Any person under the age of 18. | Age of majority, Age of sexual consent, Minor, Juvenile, Adolescent, Teenager, Young person/young people/youth | pp. 5–6 |
| Child in the online environment | A child is any person under the age of 18, whether she/he is acting in the online environment or offline. Protection from sexual exploitation and sexual abuse should not be lessened by the fact that a child is acting online. | Child, Age of majority, Age of sexual consent, Minor, Juvenile, Adolescent, Teenager, Young person/young people/youth | p. 11 |
| Child pornography | “(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct; (ii) any depiction of the sexual organs of a child for primarily sexual purposes; | Child sexual abuse material/child sexual exploitation material, Computer/digitally generated child sexual abuse material, Sexualised images of children/child erotica, | pp. 35–38 |

| Term | Definition | Other related terms | Guidance |
|---------------------------|--|---|--------------|
| | <p>(iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or (iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes”. Colloquial terms to refer to child pornography (e.g. “child porn”, “kiddy porn”, or “paedo-porn”) should be avoided.</p> | <p>Self-generated sexual content/ material, Sexting, (Exposure to) harmful content, Corruption of children for sexual purposes</p> | |
| <p>Child Prostitute</p> | <p>Should never be used in legislative or Child policy documents or in practice, as it may harm the child and/or risk shifting the blame onto the child.</p> | <p>Exploitation of children in/for prostitution, Children in (a situation of) prostitution, Child sex worker, Children/adolescents/young people selling sex, Voluntary/self- engaged prostitution, Transactional sex, Use of children for pornographic performances</p> | <p>p. 31</p> |
| <p>Child sex offender</p> | <p>The term “child sex offender” is one of the most frequently used terms to refer specifically to individuals involved in sex-based crimes against children, and it is particularly used by international law enforcement agencies. The term encompasses all forms of sexual offences against children, including acts carried out through or enabled by the Internet.</p> | <p>Perpetrators of sexual crimes against children, Sex offender, Preferential offenders, Situational offenders, Transnational child sex offenders, Travelling child sex offenders, Child sex tourist, Juvenile sex offender, Facilitator, Customer/client/John</p> | <p>p. 85</p> |
| <p>Child sex tourism</p> | <p>Sexual exploitation of children in the context of travel and tourism</p> | <p>Sexual exploitation of children in the context of travel and tourism</p> | <p>p. 56</p> |
| <p>Child sex tourist</p> | <p>Like “child sex tourism”, the term “child sex tourist” is frequently used to refer to tourist travelling perpetrators of child sexual offences. The term should be avoided.</p> | <p>Perpetrators of sexual crimes against children, Sex offender, Child sex offender, Preferential offenders, Transnational child sex offenders, Travelling child sex offenders, Travelling child sex offenders, Juvenile sex offender, Facilitator, Customer/ client/John</p> | <p>p. 89</p> |
| <p>Child sex worker</p> | <p>Should never be used to refer to children sexually exploited through prostitution, since they could imply that this is a legitimate occupation for a child, or shift the blame onto the child.</p> | <p>Exploitation of children in/for prostitution, Children in (a situation of) prostitution, Child prostitute, Children/adolescents/young people selling sex, Voluntary/self-engaged prostitution, Transactional sex, Use of children for pornographic performances</p> | <p>p. 31</p> |

| Term | Definition | Other related terms | Guidance |
|--|---|--|------------------|
| Child sexual abuse | “(a) engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities” 81 and: “(b) engaging in sexual activities with a child where: use is made of coercion, force or threats; or abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.” | Incest, Rape of a child, Child sexual molestation, Sexual touching of children, Sexual harassment of a child, Online child sexual abuse | pp. 18–20 |
| Child sexual abuse material/ child sexual exploitation material | The term “child sexual abuse material” is increasingly being used to replace the term “child pornography”. This switch of terminology is based on the argument that sexualised material that depicts or otherwise represents children is indeed a representation, and a form, of child sexual abuse, and should not be described as “pornography”. | Child pornography, Computer/digitally generated child sexual abuse material, Sexualised images of children/child erotica, Self-generated sexual content/material, Sexting, (Exposure to) harmful content, Corruption of children for sexual purposes | pp. 38–40 |
| Child sexual abuse to order | A specific type of online sexual abuse that consists of a perpetrator requesting or dictating beforehand—or while the abuse takes place—that a certain action be carried out. | Live online child sexual abuse, Live streaming of child sexual abuse, Webcam child sex tourism/webcam child sex abuse | pp. 47–48 |
| Child sexual assault | “Sexual assault” is defined as “the action or an act of forcing an unconsenting person to engage in sexual activity; a crime involving forced sexual contact” or “sexual contact that usually involves force upon a person without consent”. ” | Sexual violence against children | p. 17 |
| Child sexual exploitation | A child is a victim of sexual exploitation when she/he takes part in a sexual activity in exchange for something (e.g. gain or benefit, or even the promise of such) from a third party, the perpetrator, or by the child her/himself. | Commercial sexual exploitation of children, Online child sexual exploitation | pp. 24–25 |
| Child sexual molestation | Molestation refers to the act of touching or attacking someone, especially a child, in a sexual way. | Child sexual abuse, Incest, Rape of a child, Sexual touching of children, Sexual harassment of a child, Online child sexual abuse | p. 21 |

| Term | Definition | Other related terms | Guidance |
|--|---|--|-----------|
| Child victim of sexual exploitation and/or abuse | “Children and adolescents, under the age of 18, who are victims of crime [...] regardless of their role in the offence or in the prosecution of the alleged offender or groups of offenders.” | Victim identification, Survivor, Children subjected to sexual exploitation/sexual abuse, Victimization, Self-victimisation, Re-victimisation, Secondary victimisation | pp. 77–78 |
| Child/early marriage | Child marriage is a marriage in which at least one of the parties is a child. It also refers to the act of marrying off children, usually young girls, with or without their consent. | Forced marriage, Teenage marriage, Temporary marriage | pp. 62–64 |
| Children in (a situation of) prostitution | This term refers more to the situation or living conditions of a child, indicating that there are cases in which children find themselves in prostitution, or that the child is living in an environment of prostitution without being sexually exploited her/himself. | Exploitation of children in/for prostitution, Child prostitute, Child sex worker, Children/adolescents/young people selling sex, Voluntary/self-engaged prostitution, Transactional sex, Use of children for pornographic performances | pp. 30–31 |
| Children subjected to sexual exploitation/sexual abuse | Alternative term for victim or survivor. The expression “children subjected to sexual exploitation or abuse” describes a situation in a more neutral fashion without labelling the child with a noun. At the same time, the term clearly denotes that the responsibility does not lie with the child but with the person who subjected the child to the exploitation/abuse. | Child victim of sexual exploitation and/or abuse, Victim identification, Survivor, Victimization, Self-victimisation, Re-victimisation, Secondary victimisation | p. 81 |
| Children/adolescents/young people selling sex | Children should not be referred to as persons “selling sex”, reference should always be made to the fact that they are sexually exploited. | Exploitation of children in/for prostitution, Children in (a situation of) prostitution, Child prostitute, Child sex worker, Voluntary/self-engaged prostitution, Transactional sex, Use of children for pornographic performances | p. 32 |
| Commercial sexual exploitation of children | A form of sexual exploitation where the focus is specifically on monetary benefit, often relating to organised criminality where the primary driver is economic gain. | Child sexual exploitation, Online child sexual exploitation | pp. 26–27 |
| Computer/digitally generated child sexual abuse material | Computer-generated child sexual abuse material is the production, through digital media, of child sexual abuse material and other wholly or partly artificially or digitally created sexualised images of children. This type of material is also commonly referred to as “virtual child | Child pornography, Child sexual abuse material/child sexual exploitation material, Sexualised images of children/child erotica, Self-generated sexual content/material, Sexting, (Exposure to) harmful content, Corruption of children for sexual purposes | pp. 40–41 |

| Term | Definition | Other related terms | Guidance |
|---|--|---|-----------|
| Contemporary forms of slavery/ child slavery | <p>pornography’ or “pseudo child pornography”..”.</p> <p>While a broad range of child sexual exploitation and sexual abuse have been labelled “slavery” and constitute a violation of the international legal framework on slavery, it must be recalled that the notion of slavery is much wider and encompasses human rights violations against both children and adults. Furthermore, slavery is far from limited to sexual violence, and can include forced labour and trafficking for other than sexual purposes.</p> | N/A | pp. 71–73 |
| Corruption of children for sexual purposes | <p>Acts causing the child to witness sexual abuse or sexual activities. “Online sexual corruption of a child” is sometimes used in legal standards as an alternative term to “online solicitation of children for sexual purposes” (“grooming”).</p> | Child pornography, Child sexual abuse material/child sexual exploitation material, Computer/ digitally generated child sexual abuse material, Sexualised images of children/child erotica, Self- generated sexual content/material, Sexting, (Exposure to) harmful content | p.45 |
| Customer/ client/John | <p>Persons who pay to sexually abuse children for their own gratification are frequently referred to as “customers” or “clients”, or sometimes as “Johns”. They completely omit the fact that child sexual exploitation is a criminal act and a serious violation of the child’s human rights, and are thus inappropriate in this context.</p> | Perpetrators of sexual crimes against children, Sex offender, Child sex offender, Preferential offenders, Transnational child sex offenders, Travelling child sex offenders, Child sex tourist, Juvenile sex offender, Facilitator | p. 90 |
| Exploitation of children in/for prostitution | <p>The use of a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment in exchange for the child engaging in sexual activities, regardless of whether that payment, promise or consideration is made to the child or to a third party.</p> | Children in (a situation of) prostitution, Child prostitute, Child sex worker, Children/adolescents/ young people selling sex, Voluntary/ self-engaged prostitution, Transactional sex, Use of children for pornographic performances | pp. 29–30 |
| Exposure to harmful content | <p>Exposure to harmful content refers to children accessing or being exposed to, intentionally or incidentally, age-inappropriate sexual or violent content, or content otherwise considered harmful to their development. “Harmful content” does not necessarily refer only to illegal material but can also include material</p> | Child pornography, Child sexual abuse material/child sexual exploitation material, Computer/ digitally generated child sexual abuse material, Sexualised images of children/child erotica, Self- generated sexual content/material, Sexting, Corruption of children for sexual purposes | pp. 44–45 |

| Term | Definition | Other related terms | Guidance |
|---|--|---|-----------|
| | that is legal but still harmful to a person considering his/her age, level of maturity, etc. | | |
| Facilitator | As explained in the interpretive section above, the term “facilitator” (also known as the “intermediary”) refers to the individual whose conduct facilitates or aids and abets the (sometimes commercial) contact sexual offence against the child. The facilitator may be, but is not necessarily, the person who receives the benefit or payment for the sexual exploitation of a child. | Perpetrators of sexual crimes against children, Sex offender, Child sex offender, Preferential offenders, Transnational child sex offenders, Travelling child sex offenders, Child sex tourist, Juvenile sex offender, Customer/client/John | pp. 89–90 |
| Forced marriage | A forced marriage is a marriage to which one or both of the spouses did not give her/his/their free or full consent or is/are not able to owing to lack of maturity and/or capacity. | Child/early marriage, Teenage marriage, Temporary marriage | pp. 65–66 |
| Grooming (online/offline) for sexual purposes | The short name for the solicitation of children for sexual purposes. “Grooming/online grooming” refers to the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person. | Solicitation of children for sexual purposes, Online (sexual) enticement of children, Sexual extortion of children | pp. 51–52 |
| Harmful practices | Harmful practices are often linked to child and early marriage, 305 but also include other practices that are seen as harmful to the child, such as corporal punishment and female genital mutilation/cutting. | N/A | pp. 68–70 |
| Incest | The sexual activity between two people who are very closely related in a family, for example siblings, or parent and child. Incest involving a child constitutes sexual abuse. | Child sexual abuse, Rape of a child, Child sexual molestation, Sexual touching of children, Sexual harassment of a child, Online child sexual abuse | p. 20 |
| Juvenile | “Juvenile” is another frequently used term to refer to persons under the age of 18, often used in the context of criminal justice. | Child, Age of majority, Age of sexual consent, Minor, Adolescent, Teenager, Young person/young people/youth | p. 9 |
| Juvenile sex offender | The term “juvenile sex offender” is used for persons under the age of 18 years who under their national law are considered criminally responsible for | Perpetrators of sexual crimes against children, Sex offender, Child sex offender, Preferential offenders, Transnational child sex offenders, | p. 89 |

| Term | Definition | Other related terms | Guidance |
|---|--|--|------------------|
| | sexual offences and have been convicted. | Travelling child sex offenders, Child sex tourist, Facilitator, Customer/client/John | |
| Live online child sexual abuse | “Live exhibition aimed at an audience, including by means of information and communication technology, of (i) a child engaged in real or simulated sexually explicit conduct; or (ii) the sexual organs of a child for primarily sexual purposes” ..”. | Live streaming of child sexual abuse, Child sexual abuse to order, Webcam child sex tourism/webcam child sex abuse | pp. 46–47 |
| Live streaming of child sexual abuse | Live online child sexual abuse transmitted instantaneously to the viewer, who can watch and engage while the abuse is occurring. Streaming leaves no trace on the device, because no file is downloaded; when the streaming is stopped the child sexual abuse material is gone, unless the offender deliberately records it. | Live online child sexual abuse, Child sexual abuse to order, Webcam child sex tourism/webcam child sex abuse | p. 47 |
| Minor | [Legal Term] A person who is “under the age at which you legally become an adult”—that is, who has not attained the age of majority—which could be attained before (or after) the age of 18 depending on the legislation of each country. | Child, Age of majority, Age of sexual consent, Juvenile, Adolescent, Teenager, Young person/young people/youth | pp. 8–9 |
| Online (sexual) enticement of children | Enticement of children is sometimes used as a synonym of the “solicitation of children for sexual purposes” or “grooming”. | Solicitation of children for sexual purposes, Grooming (online/offline) for sexual purposes, Sexual extortion of children | p. 52 |
| Online child sexual abuse | The term “online child sexual abuse” has become a widely used term to refer both to the sexual abuse of children that is facilitated by ICTs (e.g. online grooming) and to sexual abuse of children that is committed elsewhere and then repeated by sharing it online through, for instance, images and videos (which is where it becomes exploitation, see Section D.4.II on “online child sexual exploitation”). The preferred term in the case of the former is “online-facilitated child sexual abuse”. | Child sexual abuse, Incest, Rape of a child, Child sexual molestation, Sexual touching of children, Sexual harassment of a child | pp. 22–23 |
| Online child sexual exploitation | Any use of ICT that results in sexual exploitation or causes a child to be sexually exploited or that results in or | Child sexual exploitation, Commercial sexual exploitation of children | pp. 27–28 |

| Term | Definition | Other related terms | Guidance |
|---|---|---|-----------|
| Perpetrators of sexual crimes against children | causes images or other material documenting such sexual exploitation to be produced, bought, sold, possessed, distributed, or transmitted. “Offender” and “perpetrator” tend to be the most frequently used terms to refer to individuals having allegedly committed or been convicted of committing sexual offences against children. | Sex offender, Child sex offender, Preferential offenders, Situational offenders, Transnational child sex offenders, Travelling child sex offenders, Child sex tourist, Juvenile sex offender, Facilitator, Customer/client/John | pp. 83–84 |
| Preferential offenders | Individuals with a predisposition or motivation to sexually engage with children and who seek out children for sexual interaction have been described as “preferential offenders”. They have identifiable behavioural traits and their offending tends to lie within the spectrum of sexually deviant paraphilias. | Perpetrators of sexual crimes against children, Sex offender, Child sex offender, Situational offenders, Transnational child sex offenders, Travelling child sex offenders, Child sex tourist, Juvenile sex offender, Facilitator, Customer/client/John | pp. 86–87 |
| Rape of a child | Rape is the crime of forcing someone (in this case a child) to have sex against her or his will, and it often involves the use of physical force or violence. It is important when using this term, to ensure that it is used in a gender- neutral manner. | Child sexual abuse, Incest, Child sexual molestation, Sexual touching of children, Sexual harassment of a child, Online child sexual abuse | p. 20 |
| Revictimisation | Refers to a pattern wherein the victim of abuse and/or crime has a statistically higher tendency to be victimised again, either shortly thereafter or much later in adulthood in the case of abuse as a child. | Child victim of sexual exploitation and/or abuse, Victim identification, Survivor, Children subjected to sexual exploitation/sexual abuse, Victimization, Self- Victimization, Secondary victimisation | pp. 81–82 |
| Sale of children | “Sale of children means any act or transaction whereby a child is transferred by any person or group of persons to another for remuneration or any other consideration”. “(a) In the context of sale of children as defined in article 2: (i) Offering, delivering or accepting, by whatever means, a child for the purpose of: a. Sexual exploitation of the child; b. Transfer of organs of the child for profit; c. Engagement of the child in forced labour; (ii) Improperly inducing consent, as an | N/A | pp. 57–58 |

| Term | Definition | Other related terms | Guidance |
|---|--|--|-----------|
| intermediary, for the adoption of a child in violation of applicable international legal instruments on adoption”. | | | |
| Secondary victimisation | The term “secondary victimisation” relates to further victimisation following on from the original (sexual) victimisation. It has been defined as “[t]he victim-blaming attitudes, behaviour, and practices engaged in by community service providers, which results in additional trauma for sexual assault survivors” or as the negative social or societal reaction or consequence of the primary victimisation, which the victim experiences as a further violation. | Child victim of sexual exploitation and/or abuse, Victim identification, Survivor, Children subjected to sexual exploitation/sexual abuse, Victimization, Self- Victimization, Re-victimisation | p. 82 |
| Self-Victimisation | Children cannot consent to their own exploitation or abuse by another. Therefore, to use the term “self-victimisation” in the field of sexual abuse and exploitation of children, which could infer that the child is responsible or to blame for the crime she/he has suffered, would be inappropriate. | Child victim of sexual exploitation and/or abuse, Victim identification, Survivor, Children subjected to sexual exploitation/sexual abuse, Victimization, Re-victimisation, Secondary victimisation | p. 81 |
| Self-generated sexual content/material | Material or content is self-generated (whether illegal or not, and whether coerced or not); sexualised (but leaving aside indecent, which may involve a more subjective value judgement); and involving children. | Child pornography, Child sexual abuse material/child sexual exploitation material, Computer/digitally generated child sexual abuse material, Sexualised images of children/child erotica, Sexting, (Exposure to) harmful content, Corruption of children for sexual purposes | pp. 43–44 |
| Sex offender | The term “sex offender” refers to a person who is involved in or has committed a crime of a sexual nature. | Perpetrators of sexual crimes against children, Child sex offender, Preferential offenders, Situational offenders, Transnational child sex offenders, Travelling child sex offenders, Child sex tourist, Juvenile sex offender, Facilitator, Customer/client/John | pp. 84–85 |
| Sexting | Sexting is a commonly used term, and a frequent practice among young persons. It is often a consensual activity between peers, although research has shown that girls feel pressured or coerced into it more often than boys. When sexting leads | Child pornography, Child sexual abuse material/child sexual exploitation material, Computer/digitally generated child sexual abuse material, Sexualised images of children/child erotica, Self-generated sexual content/material, (Exposure to) | p. 44 |

| Term | Definition | Other related terms | Guidance |
|---|---|---|-------------------|
| | to abuse or exploitation, it is crucial that the fact that the material is self-generated does not result in blaming the child for what happens or in holding the child criminally liable for the production of child sexual abuse material. | harmful content, Corruption of children for sexual purposes | |
| Sexual exploitation of children in the context of travel and tourism | The sexual exploitation of children by a person or persons who travel from their usual environment to a destination abroad where they have sexual contact with children”. “Child sex tourism can be facilitated by travel agencies operating on the Internet as they enable the exchange of information and planning of sex tourism activities.” | Child sex tourism | pp. 54–56 |
| Sexual extortion of children | Where a child is coerced into continuing to produce sexual material and/or told to perform distressing acts under threat of exposure to others of the material that depicts them. | Solicitation of children for sexual purposes, Grooming (online/offline) for sexual purposes, Online (sexual) enticement of children | pp. 52–53 |
| Sexual harassment of a child | Any form of unwanted verbal, non-verbal, or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating, or offensive environment. | Child sexual abuse, Incest, Rape of a child, Child sexual molestation, Sexual touching of children, Online child sexual abuse | pp. 21–22 |
| Sexual touching of children | Sexual touching of a child is a form of sexual abuse. “To touch” means to physically put hands on something or someone, and the term “sexual touching of children” mainly refers to the act of touching the private parts of a child’s body, and/or making the child touch her or his own private parts, for the purpose of one’s own sexual arousal/gratification. | Child sexual abuse, Incest, Rape of a child, Child sexual molestation, Sexual harassment of a child, Online child sexual abuse | p. 21 |
| Sexual violence against children | Sexual violence against children encompasses both sexual exploitation and sexual abuse of children and can be used as an umbrella term to refer jointly to these phenomena, both with regard to acts of commission and omission and associated to physical and psychological violence. | Child sexual assault | pp. 12– 17 |

| Term | Definition | Other related terms | Guidance |
|--|---|---|-----------|
| Sexualised images of children/child erotica | “Child erotica” consists of images of children posing semi-nude or nude with the emphasis on sexualising the child. Where there is a clear sexualisation of the child in the images, it is recommended to use the term CSEM. | Child pornography, Child sexual abuse material/child sexual exploitation material, Computer/digitally generated child sexual abuse material, Self-generated sexual content/material, Sexting, (Exposure to) harmful content, Corruption of children for sexual purposes | p. 42 |
| Situational offenders | Individuals who do not display any distinguishable sexual preference for children or adolescents but who will engage in the sexual exploitation of children if and when they find themselves in situations where a child is readily available for sexual use. “Situational sex offenders” frequently molest readily available children to whom they have easy access, such as their own or those they may live with or have control over. | Perpetrators of sexual crimes against children, Sex offender, Child sex offender, Preferential offenders, Transnational child sex offenders, Travelling child sex offenders, Child sex tourist, Juvenile sex offender, Facilitator, Customer/client/John | pp. 87–88 |
| Solicitation of children for sexual purposes | The solicitation of children for sexual purposes is often referred to as “grooming” or “online grooming”. It can be described as a practice by means of which an adult “befriends” a child (often online, but offline grooming also exists and should not be neglected) with the intention of sexually abusing her/him. | Grooming (online/offline) for sexual purposes, Online (sexual) enticement of children, Sexual extortion of children | pp. 49–51 |
| Survivor | The terms survivor or victim are often used interchangeably, the term “survivor” is sometimes preferred outside of legal and medical contexts, for instance in the psychological and social support sectors, because the term “survivor” implies resilience. | Child victim of sexual exploitation and/or abuse, Victim identification, Children subjected to sexual exploitation/sexual abuse, Victimization, Self-victimisation, Re-victimisation, Secondary victimisation | p. 80 |
| Teenage marriage | “Teenage marriage” is an often-used term to differentiate the marriage between younger children and that of teenagers (13–19 years old). Since it can include persons who have attained the age of majority (persons up to 19 years of age) this term cannot be considered a synonym for child marriage. | Child/early marriage, Forced marriage, Temporary marriage | p. 66 |
| Teenager | A person between 13 and 19 years of age. | Child, Age of majority, Age of sexual consent, Minor, Juvenile, Adolescent, Young person/young people/youth | p. 10 |

| Term | Definition | Other related terms | Guidance |
|---|---|---|-----------|
| Temporary marriage | The term “temporary marriage” refers to short-term contract marriages that often serve as an excuse to cover up or condone sexual exploitation or abuse. | Child/early marriage, Forced marriage, Teenage marriage | p. 67 |
| Trafficking of children | Child trafficking is the recruitment and/or transport, transfer, harbouring, and receipt of a child by others with the intent of exploiting the child through various means, like prostitution, begging, child labour, etc. | N/A | pp. 59–61 |
| Transactional sex | Within the field of protection of children from sexual exploitation, this terminology would not be the most appropriate, as it would risk (inadvertently or not) legitimising certain forms of child sexual exploitation. | Exploitation of children in/for prostitution, Children in (a situation of) prostitution, Child prostitute, Child sex worker, Children/ adolescents/ young people selling sex, Voluntary/ self-engaged prostitution, Use of children for pornographic performances | pp. 32–34 |
| Transnational child sex offenders | The term “transnational child sex offender” is used to refer to a national or permanent resident who travels or resides in another country and sexually exploits a child, regardless of her/his status and of the circumstances of her/his travel/ residence. | Perpetrators of sexual crimes against children, Sex offender, Child sex offender, Preferential offenders, Transnational child sex offenders, Travelling child sex offenders, Child sex tourist, Juvenile sex offender, Facilitator, Customer/client/John | p. 88 |
| Travelling child sex offenders | A “travelling child sex offender” has been defined as a person who travels in order to commit sexual offences against children. Some law enforcement agencies still use the term “travelling sex offenders” but it has been increasingly replaced by the above- discussed term “transnational child sex offenders”, which is seen as broader. | Perpetrators of sexual crimes against children, Sex offender, Child sex offender, Preferential offenders, Transnational child sex offenders, Travelling child sex offenders, Child sex tourist, Juvenile sex offender, Facilitator, Customer/client/John | pp. 88–89 |
| Use of children for pornographic performances | The “use of children for pornographic performances” extends the notion of “pornographic” to cover not only what is recorded and/or documented but also what is performed live. | Exploitation of children in/for prostitution, Children in (a situation of) prostitution, Child prostitute, Child sex worker, Children/ adolescents/ young people selling sex, Voluntary/ self-engaged prostitution, Transactional sex | p. 34 |
| Victim identification | The term “victim identification” refers to an investigation process by experts to analyse CSAM/CSEM (child sexual | Child victim of sexual exploitation and/or abuse, Survivor, Children subjected to sexual exploitation/ | pp. 78–79 |

| Term | Definition | Other related terms | Guidance |
|--|---|--|-----------|
| | abuse material/child sexual exploitation material) in order to identify the victims of sexual abuse or sexual exploitation. A victim-centred discipline within policing and should be included as a constituent part in any child exploitation investigation. | sexual abuse, Victimization, Self-victimisation, Re- victimisation, Secondary victimisation | |
| Victimisation | The term “victimisation” refers to the act of victimising someone; singling (someone) out for cruel or unjust treatment. The sexual exploitation and sexual abuse of children represent forms of victimisation, whereby the child is the victim of the exploitation/ abuse. | Child victim of sexual exploitation and/or abuse, Victim identification, Survivor, Children subjected to sexual exploitation/sexual abuse, Self-victimisation, Re-victimisation, Secondary victimisation | p. 81 |
| Voluntary/ self-engaged prostitution | With regard to children involved in prostitution, the terms “voluntary” and “self-engaged” should be avoided. Children under the age of 18 years who are involved in prostitution should always be seen and addressed as victims of sexual exploitation. | Exploitation of children in/for prostitution, Children in (a situation of) prostitution, Child prostitute, Child sex worker, Children/ adolescents/ young people selling sex, Transactional sex, Use of children for pornographic performances | p. 32 |
| Webcam child sex tourism/ webcam child sex abuse | The term “webcam child sex tourism” should be avoided. The term “webcam child sex abuse” can be used bearing in mind that it refers to a specific technological device and that “live online child sexual abuse” is broader and may be more appropriate. | Live online child sexual abuse, Live streaming of child sexual abuse, Child sexual abuse to order | p. 48 |
| Worst forms of child labour | Even where they are not directly used for purposes of sexual exploitation as defined by ILO C182 Article 3(b), children who are working (whether in child labour or as young workers of legal working age) are vulnerable to and run an elevated risk of being exposed to different forms of sexual violence and abuse in the workplace. | N/A | pp. 74–76 |
| Young person/ young people/ youth | UN: The 15–24-year-old age group. African Youth Charter: 15–35-year-old age group. | Child, Age of majority, Age of sexual consent, Minor, Juvenile, Adolescent, Teenager | pp. 10–11 |

APPENDIX D: REPORT ON GOVERNMENT OF RWANDA VISIT TO POLICE SCOTLAND

PURPOSE

The purpose of this report is to provide some information in relation to a study visit to Police Scotland carried out by the Government of Rwanda from Monday 4th March to Friday 8th March 2019 inclusive.

Specifically, this report will provide an overview of the subject matters covered, some commentary on the usefulness of the visit and some suggestions for taking matters forward. This report is not intended to detail all activity, nor can it provide detailed proposals as it was both short in duration and by necessity limited in depth. Nevertheless, it may be useful to consider along with other material that will be available.

The close co-operation and generosity of both 5Rights Foundation and the Scottish Government is acknowledged as being vital to the study visit being possible.

INTRODUCTION

Both the Scottish Government and Police Scotland had previous working relationships with the Government of Rwanda, the Scottish Government in a range of areas and Police Scotland in terms of support specifically to issues relating to Gender Based Violence.

Having been contacted by 5Rights Foundation, Police Scotland agreed to collaborate on the delivery of a five-day study visit in order to showcase both offline and online Child Protection strategies. Five members of the Rwandan Government attended at Police Scotland Headquarters (also the Scottish Police College), Tulliallan Castle, with four members of the delegation arriving on Monday 4th March and the fifth arriving on Tuesday 5th March 2019.

Police Scotland's International Development and Innovation Unit, under its Head of Unit John Wyllie hosted the delegation with the Executive lead being Deputy Chief Constable Will Kerr. The study visit focussed on a number of "themed" days as follows.

Day 1: Introductions and Overview

This was designed to orientate delegates to Tulliallan, general approaches to policing in Scotland, specifically the focus on community engagement and partnership working, the GIRFEC (Getting It Right For Every Child) system and how Scotland policing is structured nationally, regionally and locally. This was designed to provide context to the rest of the week. See *Figure 7*.

Day 2: National Capabilities

Delegates were transported to the Scottish Crime Campus, Gartcosh which is home to a variety of UK Law Enforcement agencies, operating in a co-located facility, which is without doubt the most advanced of its type in the UK. Detailed presentations were provided in three areas : firstly the National Child Abuse Investigation Units inception, structure and remit and the ongoing review of Child Protection in Scotland ; secondly approaches and practice of preventing on-line child abuse, through Police Scotland's National Safer Communities approach; and thirdly from Police Scotland National Cyber Team on the UK National Child Abuse Identification Database, the National On Line Child Abuse Package (NOCAP) system which delivers intelligence packages to local enforcement teams and Cyber Forensics (the forensic investigation of ICT hardware). This was day was specifically aimed at showcasing the type of capability that would be required at a National Law Enforcement level.



The Scottish Police College. This was the main centre of delivery for the week and is both the Headquarters of Police Scotland and its main training centre.

Day 3: Partnerships

Delegates were hosted at the Scottish Police College, Tulliallan where they were shown presentations on the collection of and legislation governing police powers in relation to the obtaining of Communications Data. This is vital in on-line investigations and can provide evidence of device use, positional data, signing into Wi-Fi and internet and communication with other devices. The obtaining of Communications Data does not require the seizure of hardware. This requires Law Enforcement, Criminal Justice System and Internet/Communications Service Provider co-operation and a legislative framework to balance the rights of individuals with the powers of the state. The Scottish approach to public and private sector partnerships was demonstrated by examining the Scottish Business Resilience Centre, a model that is being replicated in other parts of the UK to provide access to cutting edge Cyber capabilities in a way that protects the public, businesses and individuals. The overall aim of the day was to demonstrate the vital role that partnerships across Government, statutory agencies such as the police, education, health and social work, businesses and individuals play in preventing harm and protecting people.



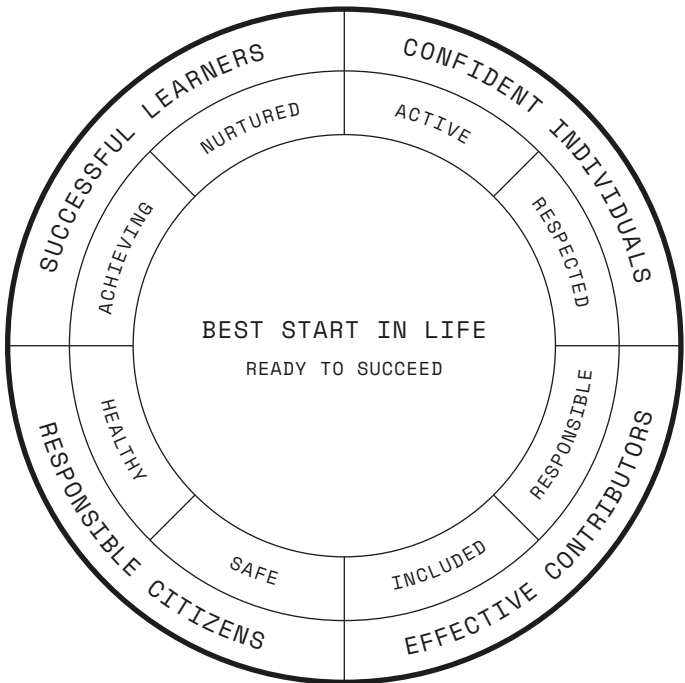
Livingston Civic Centre. This multi-agency site is perhaps the best example of co-location of statutory services in the UK and was the delivery site for day four of the programme.

286 See, <https://www.weprotect.org/the-model-national-response>

Figure 7

THE SHANARRI WHEEL

This shows the various indicators used in GIRFEC (Getting It Right For Every Child) which are then used to monitor the services provided by police, education, social work, health and all other parties to child protection. In short it is everyone's job to protect children.



NURTURED

Having a nurturing place to live, in a family setting with additional help if needed or, where this is not possible, in a suitable care setting.

RESPONSIBLE

Having opportunities and encouragement to play active and responsible roles in their schools and communities and, where necessary, having appropriate guidance and supervision and being involved in decisions that affect them.

ACHIEVING

Being supported and guided in their learning and in the development of their skills, confidence and self-esteem at home, at school and in the community.

INCLUDED

Having help to overcome social, educational, physical and economic inequalities and being accepted as part of the community in which they live and learn.

ACTIVE

Having opportunities to take part in activities such as play, recreation and sports which contribute to healthy growth and development, both at home and in the community.

RESPECTED

Having the opportunity, along with carers, to be heard and involved in decisions which affect them.

SAFE

Protected from abuse, neglect or harm at home, at school, and in the community.

HEALTHY

Having the highest attainable standards of physical and mental health, access to suitable healthcare, and support in learning to make healthy and safe choices.

Day 4: Operational Service Delivery

Delegates were transported to Livingston Civic Centre. This is a multi-agency facility in West Lothian, 10 miles West of Edinburgh. The facility hosts West Lothian Council Headquarters, the Local Government area covering a population of around 400,000 people, and contains a police station, social work, education, housing, fire service and law Courts. Delegates took part in presentations on the developments of dedicated police on-line child protection teams, operational enforcement, processes for dealing with victims, witnesses and suspects, forensic facilities and custody facilities including suspect interview rooms. This was designed to show the cutting edge of enforcement, whilst again emphasising the need for a multi-agency approach.

That evening the Rwandan guests and Baroness Kidron were treated to a traditional Scottish dinner, with traditional bagpipe music and food. Police Scotland prides itself as an organisation that is welcoming and that seeks to engage in keeping people safe globally as well as locally so the evening was a chance to demonstrate “Global Citizenship” in action.



Global Citizens. This photograph, taken in the main reception area of Tulliallan Castle shows the Global Partnership of the Rwandan Government, 5Rights Foundation, Police Scotland and the Scottish Government – colleagues and friends working together to help prevent and combat on-line child abuse.

Day 5: Reflection and Discussion

This day involved a detailed and structured discussion of the weeks’ activities in the context of designing an overall programme of work to ensure a practical and effective strategic approach to the on-line abuse of children. The day was jointly facilitated by 5Rights Foundation and Police

Scotland and provided delegates with the opportunity to consider a range of approaches across the public, private and third sectors, supported by evidence of an operating system. Effectively the discussion ranged across the elements of the #WePROTECT Model National Response covering many of the areas, further information on which can be found online.²⁸⁶

Future Steps

In order to build upon this visit and in connection with wider work being undertaken by 5Rights Foundation in order to develop a national strategy with the Rwandan Government there are a number of future steps that could be developed. This document is not intended to be prescriptive and what is hereafter suggested as worthy of consideration is based upon the professional judgement of the author, both in terms of experience in this area in service, policy development and training delivery nationally and internationally, including in current programmes in sub-Saharan Africa.

Consider the current capabilities of “off-line” Child Protection services in Rwanda. This would include the national strategic approach, the specific duties, capabilities and capacity of the statutory agencies, including police, health, social care and education.

This consideration would almost certainly require a Training Needs Assessment, based upon any Strategic Threat and Risk Assessment that is already in place or under development.

Consider an immediate focus on prevention to limit harm and provide a safer space for other capabilities to develop. This would include Governmental expectations for Internet and Communication Service Providers and might involve licensing arrangements for service provision being reviewed against Governmental requirements.

For law enforcement a detailed examination of capability and capacity in terms of ability to access Communications Data and to undertake Digital Forensics. Crime scene management, investigative interviewing and investigative management may also link into this examination.

It is extremely difficult to gauge capability and capacity based upon a 5-day engagement so this paper will not attempt to do so but what was clear from the delegates is that there is a clear desire and determination to tackle on-line Child Protection.

As signatories to and very active participants in the Kigali International Convention Declaration (KICD) the Government of Rwanda, who host the Centre of Excellence of excellence for KICD, have an opportunity to lead the way in this area, if suitably supported to do so.

John Wyllie

*Head of International Development and Innovation Unit,
Police Scotland, 2nd May 2019*

APPENDIX E: A REVIEW OF ONLINE CHILD PROTECTION LAWS IN RWANDA

PROVIDED BY ABHILASH NAIR

1. INTRODUCTION

Whilst the various pieces of legislation broadly create offences criminalising the production and distribution of child sexual abuse material (CSAM), there appear to be some key omissions.

First is the issue with definitions. CSAM is not defined in the legislation, but other key terms also need clear definitions within legislation. Broader definitions are needed given the complexities of age-assessment from images, as well as in light of the challenges raised by pseudo and virtual imagery. Second, pseudo and virtual imagery call for specific legislative provisions, specifically criminalising their production, distribution, advertising and possession. Third, there is no simple possession offence for CSAM envisaged in the current laws. Apart from criminalising production and distribution, it is equally important to criminalise the intentional possession of child pornography regardless of intention to distribute further. Fourth, child grooming provisions also will benefit from clearer definitions and more widely drafted offences. Finally, more clarity on service provider liability and child trafficking provisions would strengthen the laws further.

2. DEFINITIONS

The Luxembourg terminology guidelines²⁸⁷ recommends avoiding using the term ‘child pornography’ altogether. Whilst many domestic laws and some international treaties still refer to ‘child pornography’, there is growing acceptance that the term is inappropriate to describe the sexual abuse and exploitation of children.

Alternative terminology to consider

Child sexual abuse and exploitation material. Indecent photographs/images of a child. This is a more preferred version. ‘Photographs’ and ‘images’ need to be defined clearly to include different formats, including still and moving images.

A suggested definition would be “References to an indecent photograph include an indecent film*, a copy of an indecent photograph or film, and an indecent photograph comprised in a film”

²⁸⁷ See, <http://luxembourgguidelines.org/>

²⁸⁸ See, Chapter 4, Abhilash Nair, *The Regulation of Internet Pornography: Issues and Challenges* Routledge 2018 on the rationale of this approach. The research carried out for this book underpins the advice provided in this opinion brief.

Photographs/images/films should include:

- The negative as well as the positive version
- Data stored on a computer disc (or other electronic means) capable of conversion into a photograph/image
- Tracings
- Pseudo-photographs, whether made by computer-graphics or other means, which appears to be a photograph**

*film to include still as well as moving images, any form of video recording.

**It is recommended that non-photographic sexual representations are criminalised separately as ‘virtual indecent material’ as these raise separate issues.²⁸⁸

3. SUBSTANTIVE OFFENCES & PSEUDO/VIRTUAL IMAGERY

Existing provisions on production, distribution and advertising

CHILD PROTECTION (NO 54/2011)
LAW RELATING TO THE PROTECTION OF THE CHILD
Law N°71/2018 Of 31/08/2018 Relating to the protection of the child

Arts 34-35 of the above law criminalise the creation (Art 34), advertising and distribution of child pornography (art 35), as well as showing pornographic images to a child (Art 33). There is, however, no possession offence for child pornography, which is a significant gap as noted in my general comments earlier. I have pasted the relevant articles verbatim for ease of reference, with my comments below.

ARTICLE 33

Showing a child pornographic images or sounds. A person who shows a child pornographic images or sounds commits an offence. Upon conviction, he/she is liable to imprisonment for a term of not less than five (5) years and not more than seven (7) years with a fine of not less than three million Rwandan francs (FRW 3,000,000) and not more than five million Rwandan francs (FRW 5,000,000).

Comment

This is really a separate issue as it pertains to non-child pornographic imagery and is therefore more aligned to ‘child grooming’. Whilst the offence is certainly pertinent, it sits oddly here alongside specific child pornography offences (but this is admittedly a minor point).

ARTICLE 34

Recording a child's pornographic picture or voice.

A person who, by any means records a picture or the voice of a child, if such picture or voice is of a pornographic nature commits an offence. Upon conviction, he/she is liable to imprisonment for a term of not less than five (5) years and not more than seven (7) years and a fine of not less than seven million Rwandan francs (FRW 7,000,000) and not more than ten million Rwandan francs (FRW 10,000,000).

Comment

I am not sure of the legal significance of 'recording' in Article 34 above. If it is not defined already, clear definition should encapsulate the acts of taking, making (for e.g. pseudo images), or creating CSAM in any format.

ARTICLE 35

Advertising children pornographic images. A person who displays, sells, rents, disseminates or distributes pornographic images, objects, movies, photos, slides and other pornographic materials involving children, commits an offence. Upon conviction, he/she is liable to imprisonment for a term of not less than five (5) years but not more than seven (7) years and a fine of not less than fifteen million Rwandan francs (FRW15, 000,000) and not more than twenty million Rwandan francs (FRW 20,000,000).

Comment

This is a comprehensive 'distribution offence'. A separate offence of simple possession should be introduced in the legislation (see below).

Recommendations on substantive provisions:

1 It is extremely important to specifically criminalise the simple possession (regardless of intention to distribute or gain (financial or otherwise) from the act of possession) of CSAM.

Suggested wording for the offence: It is an offence for a person to have child pornography in his or her possession.

There should be defences available on the following grounds –

- A Legitimate reason (prosecutors, police, etc.)
- B Lack of knowledge (for e.g. the person not seen the image himself, or had no reason/cause to suspect it to be indecent).
- C The image was sent unsolicited (for e.g., email attachment)

2 'Possession' to be clearly defined in the law as it can be a quite problematic to prove. For information, UK follows a concept of 'custody and control' over the image following the case of *R v Porter* [2006] EWCA Crim 560,

but this is not always easy to establish (especially where the offender accesses an image from a cybercafé without actively downloading it to the hard disk. In this instance, it will be difficult to prove that the perpetrator has custody or control of the image, which may be held in the cache of the computer owned by the cybercafé).

3 Linked to the above, it is useful to introduce an 'access offence' in the legislation, without the requirement of active downloading. This would assist with instances such as above (cybercafé); or where the perpetrator disables cache and simply views the material on their screen without actively downloading the images to their computer. It will be possible to gather evidence more effectively with the assistance of internet connection records, etc., i.e., at network level in addition to just device level.

4. GROOMING

There are some broad provisions contained within Cybercrime (No 60/2018), as below.

LAW N° 60/2018 OF 22/8/2018 ON PREVENTION AND PUNISHMENT OF CYBER CRIMES

ART 34 (2)

Art 34 (2) criminalises 'grooming' – "any person who proposes, grooms or solicits, through a computer or a computer system or any network, to meet a child for the purpose of engaging in sexual activities with the child; commits an offence"

Comment

Whilst this offence covers inappropriate communications/ sexual advances to a child, it is vague and could be problematic for successful prosecution. How is 'proposing' to be interpreted in the context of determining intention to engage in sexual activities with a child? This would of course be clear-cut where the offender makes the intention clear in the communication itself (for e.g. where the communication clearly refers to sexual activity), which in reality will not always be the case. A test of reasonableness needs to be built into the offence in terms of interpreting the nature of the communication.

ARTICLE 38

Publishing indecent information in electronic form – provides for stricter penalties when 'indecent messages' are directed to a child.

Comment

The breadth of the offence is not clear, and this is likely to be quite broad from the perspective of adults, but it should nevertheless help to address inappropriate communications directed at children.

In addition, ‘grooming’ can involve a series of communications and the law need to factor this in (for e.g. in terms of a graduated response where the intention of the offender is to lure a child by establishing trust over a series of communications before meeting up). It is also the case that predators may show CSAM or even lawful adult pornography to the child as part of the grooming process, in order to normalise this behaviour to instil false perceptions in the child to assist the offender’s motives including both physical and virtual exploitation. There is also the risk that this could lead to persuading the child to produce self-generated sexual imagery, which can then be used by the perpetrator for sexual extortion purposes. It is also prudent to incorporate an extra-territorial dimension to the offence to deter people from grooming children in foreign countries where the laws are lax.

Suggested wording for grooming offences

The following wording from s 15A of the Sexual Offences Act 2003 (SOA 2003) in the UK might offer a good reference point (this is a balanced and well drafted offence, and should work well in any jurisdiction).

1 A person aged 18 or over (A) commits an offence if—
(a) for the purpose of obtaining sexual gratification, A intentionally communicates with another person (B),
(b) the communication is sexual or is intended to encourage B to make (whether to A or to another) a communication that is sexual, and
(c) B is under 16 and A does not reasonably believe that B is 16 or over.

2 For the purposes of this section, a communication is sexual if—
(a) any part of it relates to sexual activity, or
(b) a reasonable person would, in all the circumstances but regardless of any person’s purpose, consider any part of the communication to be sexual; and
in paragraph (a) “sexual activity” means an activity that a reasonable person would, in all the circumstances but regardless of any person’s purpose, consider to be sexual.

Note – A separate offence of actually meeting/attempting to meet the child further to such communication above will be necessary to complement this. See, s 15 of the SOA 2003. Suggested wording:

A person aged 18 or over (A) commits an offence if—
 (a) A has met or communicated with another person (B) on one or more occasions and subsequently—
 (i) A intentionally meets B,
 (ii) A travels with the intention of meeting B in any part of the world or arranges to meet B in any part of the world, or
 (iii) B travels with the intention of meeting A

in any part of the world,
 (b) A intends to do anything to or in respect of B, during or after the meeting mentioned in paragraph (a)(i) to (iii) and in any part of the world, which if done will involve the commission by A of a relevant offence,
 (c) B is under 16, and
 (d) A does not reasonably believe that B is 16 or over.

5. OBLIGATIONS ON SERVICE PROVIDERS:

Notice and Takedown

There is a provision under the Cybercrime law, Article 50.

Article 50: Failure to take action on takedown notification – imposes notice and takedown obligations on ‘service providers’, which should cover CSAM, but there is no reference to any timeframe for compliance.

Suggested amendment

Insert ‘expeditiously’ after ‘takedown notification’ so that it mandates quick removal, but at the same time allows flexibility to consider all circumstances.

6. SEXUAL EXPLOITATION THROUGH TRAFFICKING

This is contained in LAW N° 51/2018 OF 13/08/2018 RELATING TO THE PREVENTION, SUPPRESSION AND PUNISHMENT OF TRAFFICKING IN PERSONS AND EXPLOITATION OF OTHERS

Comment

The law covers trafficking and exploitation of persons generally, with stricter punishment for exploitation of children under Art 24. However, a separate substantive offence specifically addressing the sexual exploitation of children via trafficking is recommended.

Article 12 contains safeguarding provisions for child victims, which is very positive.

APPENDIX F: DATA PROTECTION REGULATION RECOMMENDATION

PROVIDED BY KATHRYN CORRICK

To support Rwanda's COP policy more detailed data protection legislation is required to ensure that children's data is protected appropriately, collected only where necessary with the highest levels of security and care.

Any new data protection legislation should take into account the Rwandan context, and learn from other existing international legislation, including how children's data is categorised and protected. It should also include considerations and support for Rwanda's economic goals, technology and startup environment, so that legislation does not prevent the country's companies from reaching the highest possible standards, but bears in mind the time it takes for awareness and changes to be made within any organisation – culturally, in leadership, processes and technology.

The EU's General Data Protection Regulations currently set some of the highest standards in this area. Unlike the US's Children's Online Privacy Protection law (COPPA), which covers children under the age of 13, the EU wraps up specific protections for children into GDPR, therefore giving protection to children after they reach the age of parental consent (see below for details).

It is important to note that the rights afforded to EU citizens apply globally, meaning that technology firms wishing to enter the EU market or process EU citizen data have to adhere to the regulations accordingly. Other countries and states are updating data protection laws following the EU's lead.

Due to the scale of the EU market, the introduction of GDPR has required significant changes by multinational companies including Facebook, Google/Alphabet and Microsoft. It means that these companies now have in place changes that smaller countries would not necessarily leverage alone, to require of wealthy multinationals.

To prevent the legislation from falling too quickly behind technological developments, GDPR was written mostly as a set of principles, rather than specific rules based on current technology use. The exceptions to this are advertising tracking and algorithms used within AI.

It is for these reasons that GDPR and relating rights are suggested as a basis for Rwandan data protection policy, and also why specific technologies are referenced only occasionally, as follows:

INTRODUCE A RIGHT TO THE PROTECTION OF PERSONAL DATA

A new right to form the basis of further data protection regulations and be a reference point for individuals and organisations both locally and internationally. Showing the direction that Rwanda is headed.

For example, the Article 8 of the EU Charter on Human Rights reads:

- 1 Everyone has the right to the protection of personal data concerning him or her.
- 2 Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
- 3 Compliance with these rules shall be subject to control by an independent authority.

THE INTRODUCTION OF SPECIFIC LEGISLATION

Rwandan data protection regulations in a first phase should look to:

- Establish clear lawful bases for processing personal data, so that anything outside them is unlawful. For example, under GDPR these are: contractual, consent, legal obligation, vital interest, legitimate interest, public task.
- Establish a list of special categories of data which include children's data, but also race, health, sexual orientation, religion etc. These special categories of data would require higher levels of protection and reasons for processing.
- For digital services and products where consent is the basis for processing, establish an age before which a child is unable to provide their consent and where parental/guardian consent is required. In such cases, reasonable efforts should be required to verify that the consent has been provided by a holder of parental responsibility. Globally, where similar laws apply, this age varies, in the US and UK it is 13 years old, the default under GDPR is 16 years old.
- Review within a Rwandan context the seven GDPR principles and amend as required – these cover lawfulness and transparency, data minimisation, purpose minimisation, storage minimisation, accountability, accuracy, integrity and confidentiality (security).
- Review if adding in Data Protection by Design and Default to the list of principles or as an overriding principle, would be appropriate at this stage or whether it should be introduced later on.
- Introduce the requirement for algorithmic

transparency – that algorithms need to be explainable in what they do and data they use (this will cover much AI use)).)

- Review how additional data protection rights should work in the Rwandan context, and how they could be increased over time – as the basis of laws is different, transferring rights directly from GDPR is unlikely to be appropriate but could form the starting point for what rights Rwanda wishes to introduce and how this fits with the country’s economic goals and technology community – i.e. ideally not bringing in legislation in such a way that local technology firms are cut out, and only very large international organisations can comply.
- Review what specific privacy legislation is needed to compliment the data protection legislation – use of cookies and personal identifiers, location data, voice data, data used in IoT devices not covered by data protection, digital marketing practices not covered by data protection requirements .
- How the regulator will oversee the legislation, what powers it will be given, level of fines and other types of requests it can make to organisations, how it can work with other regulators regionally and internationally where a problem exists trans-nationally.

APPENDIX G: FURTHER READING ON THE RWANDAN CONTEXT

Regional studies identified that relate to COP:

- Apostolides, A. (2017). Cyber bullying: Child and youth spirituality. *HTS Theological Studies*, 73(3), 1-7.
- Badenhorst, C. (2011). Legal responses to cyber bullying and sexting in South Africa. *Centre for Justice and Crime Prevention (CJCP) Issue Paper*, 10, 1-20.
- Bishumba, N. (2016, May 13). Cyber bullying: Is social media becoming a poisoned chalice? Retrieved from *The New Times*: <https://www.newtimes.co.rw/section/read/199825>
- Blagbrough, J. (2010). Child domestic labour: a global concern. In G. Craig, *Child Slavery Now: A contemporary reader* (pp. 81-98). Bristol: The Policy Press.
- Bulger, M., Burton, P., O'Neill, B., & Staksrud, E. (2017). Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online. *New Media & Society*, 19(5), 750-764.
- Burton, P., & Mutongwizo, T. (2009). Inescapable violence: Cyber bullying and electronic violence against young people in South Africa. *Centre for Justice and Crime Prevention*, 8, 1-12.
- Carboni, N., & Bhana, D. (2017). Forbidden fruit: the politics of researching young people's use of online sexually explicit materials in South African schools. *Sex Education*, 17(6), 635-646.
- Chair, C. (2017, February). Internet use barriers and user strategies: Perspectives from Kenya, Nigeria, South Africa and Rwanda. (A. Gillwald, Ed.) *Beyond Access Policy Paper*, 1, 1-40. Retrieved from https://www.researchictafrica.net/docs/RIA%202016%20Comparative%20FGD%20study_Final_Web%20Version.pdf
- Chetty, I., & Basson, A. (2006). Report on Internet usage and the exposure of pornography to learners in South African schools. Retrieved through FPB website from: <http://www.fpb.org.za/research>. Houghton: Film and Publication Board. Retrieved from http://www.stop.org.za/wp-content/uploads/2011/05/FPB_Report-Porn_Exp_Children.pdf
- Chiome, C. (2015). Cyber-bullying: A new form of social cruelty in Zimbabwean schools. *Journal of Scientific Research and Reports*, 5(3), 184-193. doi:10.9734/JRRR/2015/12508
- CIA. (2019, January 28). *The World Factbook*. Retrieved from Central Intelligence Agency (CIA): <https://www.cia.gov/library/publications/the-world-factbook/geos/rw.html>
- CLADHO. (2016). Report on early/unwanted pregnancy for under 18 years in 10 districts of Rwanda. Kigali: CLADHO. Retrieved from http://www.cladho.org.rw/fileadmin/templates/document/REPORT_OF_THE_RAPID_ASSESSMENT_ON_TEENAGE_PREGNANCY.PDF
- CLADHO and IDAY-International. (2015). Domestic workers' baseline survey focusing on child domestic workers and employers in Rwanda. Kigali: CLADHO and IDAY-International. Retrieved from <http://invisibleworkers.eu/wp-content/uploads/2016/03/DWs-Baseline-Survey-Final-Report-07-015.pdf>
- De Lange, M., & von Solms, R. (2011). The importance of raising e-Safety awareness amongst children in South Africa.
- Proceedings of the 13th annual conference on world wide web applications, 14-16 September 2011. Johannesburg, South Africa: Cape Peninsula University of Technology. Retrieved from <http://www.zaw3.co.za/index.php/ZA-WWW/2011/paper/viewFile/423/131>
- Department of Basic Education. (2015, May 18). Basic Education on dangers of social media for adolescents. Retrieved from South African Government: <https://www.gov.za/speeches/sexting-spare-rod-teach-child-18-may-2015-0000>
- Ephraim, P. E. (2013). African youths and the dangers of social networking: a culture-centered approach to using social media. *Ethics and information technology*, 15(4), 275-284.
- GSMA Intelligence. (2016). *The Mobile Economy Africa 2016*. London: GSMA. Retrieved from <https://www.gsmaintelligence.com/research/?file=3bc21ea879a5b217b64d62fa24c55bdf&download>
- HAGURUKA. (2018). *HAGURUKA Annual Report 2018*. Kigali: HAGURUKA. Retrieved from http://haguruka.org.rw/wp-content/uploads/2019/02/Haguruka_Annual-Report_2018_Final.pdf
- Hakizimana, E. (2018, January 28). Why children should be aware of Cyber crimes. Retrieved from *The Inspirer*: <http://rwandainspirer.com/2018/01/28/why-children-should-be-aware-of-cyber-crimes/>
- ICO. (April 2019). *Age appropriate design: a code of practice for online services*. Wilmslow, Cheshire: ICO. Retrieved from <https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf>
- InterMedia. (2015). *Rwanda National Survey Report (December 2014-February 2015). Financial Inclusion Insights*. Retrieved from <http://finclusion.org/uploads/file/reports/FII%20Rwanda%202014%20National%20Survey%20Report.pdf>
- ITU. (2016). *Rwanda Contribution to the Council Working Group on Child Online Protection: Cyber Bullying*. ITU Headquarters, Geneva. Retrieved from <https://www.itu.int/en/council/cwg-cop/Documents/RWANDA%20CONTRIBUTION%20TO%20THE%20CWG-COP%20OCTOBER%202016.doc>
- Johnson, E. O. (2019, February 13). Rwanda poised to open Africa's first smartphone manufacturing factory in 2019. Retrieved from *face2faceafrica*: <https://face2faceafrica>.

- com/article/rwanda-poised-to-open-africas-first-smartphone-manufacturing-factory-in-2019
- Kabiawu, O., & Kyobe, M. (2015). Mobile Bullying and Victimization: A Study of Female Bully-Victims in South African High Schools. Proceedings of Second International Conference on Advances in Women's Studies 2015 (pp. 107-114). Toronto: Unique Conferences Canada.
- Kidron, B. (2018). Are children more than 'clickbait' in the 21st century? *Communications Law*, 23(1), 8-13.
- Kidron, B., Evans, A., & Afia, J. (2018). Disrupted Childhood: The Cost of Persuasive Design. London: 5Rights Foundation. Retrieved from <https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf>
- Kyobe, M. E., Mimi, L., Nembandona, P., & Mtshazi, S. (2018). Mobile bullying among rural South African students: Examining the applicability of existing theories. *The African Journal of Information Systems*, 10(2), 85-104.
- Kyobe, M. E., Oosterwyk, G. W., & Kabiawu, O. (2016). The nature of mobile bullying & victimisation in the Western Cape high schools of South Africa. *The African Journal of Information Systems*, 8(2), 45-69.
- Ladcomm Corporation. (2014). Sub-Saharan Africa Universal Service Fund study. London: GSMA. Retrieved from https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2014_Report_Sub-SaharanAfricaUniversalServiceFundStudy.pdf
- Livingstone, S., Davidson, J., Bryce, J., Batool, S., Haughton, C., & Nandi, A. (2017). Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group. London: UKCCIS. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf
- Lusinga, S., & Kyobe, M. (2017). Testing a typology of mobile phone victimisation using cluster analysis. *The Electronic Journal of Information Systems in Developing Countries*, 78(6), 1-36.
- Martellozzo, E. (2012). *Online child sexual abuse: Grooming, policing and child protection in a multi-media world*. Abingdon: Routledge.
- MIGEPROF. (2011). National Policy against Gender-Based Violence. Kigali: Ministry of Gender and Family Protection. Retrieved from https://migeprof.gov.rw/fileadmin/_migrated/content_uploads/GBV_Policy-2_1_1.pdf
- MINEDUC. (2018). 2018 Education Statistics. Kigali: Ministry of Education. Retrieved from http://mineduc.gov.rw/fileadmin/user_upload/pdf_files/2018_Rwanda_Education_Statistics.pdf
- MINICT. (2017). ICT Sector Strategic Plan (2018-2024). Kigali: Ministry of Information Technology and Communications, Republic of Rwanda. Retrieved from http://minict.gov.rw/fileadmin/Documents/Mitec2018/Policies___Publication/Strategy/ICT_SECTOR_STRATEGIC_PLAN__2018-2024_.pdf
- MITEC. (2018). ICT Hub Strategy 2024. Kigali: Ministry of Information Technology and Communications. Retrieved from http://minict.gov.rw/fileadmin/Documents/Mitec2018/Policies___Publication/Strategy/ICT_HUB_STRATEGY_FINAL.pdf
- Mothobi, O., & Rademan, B. (2017). Disentangling the broadband divide in Rwanda: supply-side vs demand-side. Cape Town: Research ICT Africa. Retrieved from https://www.researchictafrica.net/polbrf/Research ICT_Africa_Policy_Briefs/2017%20Policy%20Brief%20_Rwanda.pdf
- Ncube, L. S., & Dube, L. (2016). Cyberbullying a desecration of information ethics: Perceptions of post-high school youth in a rural community. *Journal of Information, Communication and Ethics in Society*, 14(4), 313-322.
- NISR. (2014). The Statistical Yearbook, 2014 Edition. Kigali: National Institute of Statistics of Rwanda. Retrieved from <http://statistics.gov.rw/file/3649/download?token=MrF82XaR>
- NISR. (2015). Rwanda Statistical Yearbook 2015, Chapter XIV: Law Enforcement, Court and Order. Kigali: National Institute of Statistics Rwanda. Retrieved from <http://www.statistics.gov.rw/publication/law-enforcement-court-and-order-extracts-statistical-yearbook-2015>
- NISR. (2017). Unlocking Rwanda's potential to reap the demographic dividend. Kigali: National Institute of Statistics of Rwanda. Retrieved from https://www.afidep.org/download/21.05.2018-Rwanda-DD-Report_Final-For-Print-2.pdf
- NISR. (2019, March 5). Rwanda's literacy rate rises. Retrieved from National Institute of Statistics of Rwanda: <http://statistics.gov.rw/node/1086>
- NISR, MOH & ICF International. (2015). Rwanda Demographic and Health Survey 2014-15. Rockville, Maryland, USA: National Institute of Statistics of Rwanda (NISR) [Rwanda], Ministry of Health (MOH) [Rwanda], and ICF International. Retrieved from <https://www.dhsprogram.com/pubs/pdf/FR316/FR316.pdf>
- Okoie, O. E., Nwoga, A. N., & Onah, A. T. (2015). Moderating effect of cyber bullying on the psychological well-being of in-school adolescents in Benin Edo State Nigeria. *European Journal of Sustainable Development*, 4(1), 109-118.
- Onditi, H. Z. (2017). Cyberbullying in Tanzania: adolescents' experiences and the psychosocial factors influencing coping strategies. (Doctoral dissertation, University of British Columbia).
- Phillips, K., Davidson, J., & Kidron, B. (2019). Child Online Protection in Rwanda: Implementation Plan Directory. London: University of East London and 5Rights Foundation.
- Phyfer, J., Burton, P., & Leoschut, L. (2016). Global Kids Online South Africa: barriers, opportunities and risks. A glimpse into South African children's internet use and online activities. Technical Report. Cape Town: Centre for Justice and Crime Prevention, South Africa.

- Polavarapu, A. (2011). Procuring meaningful land rights for the women of Rwanda. *Yale Human Rights and Development Journal*, 14 (1), 105-154.
- Popovac, M., & Leoschut, L. (2012). Cyber bullying in South Africa: Impact and responses. *CJCP Issue Paper*, 13, 1-16.
- Rachoene, M., & Oyedemi, T. (2015). From self-expression to social aggression: Cyberbullying culture among South African youth on Facebook. *Communication*, 41(3), 302-319.
- RURA. (2018). Rwanda Utilities Regulatory Authority (RURA) 2017-2018 Annual Report. Kigali: RURA. Retrieved from http://www.rura.rw/fileadmin/Documents/docs/report/RURA_ANNUAL_REPORT_2017-2018.pdf
- Sampson, P. D. (2014). Empowering the Future Digital Citizens. Presentation to the Africa Regional Conference on Child Online Protection. Kampala, Uganda. Retrieved from <https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Documents/Africa%20Regional%20Conf.%20On%20Child%20Online%20Protection%20%2020.pdf>
- Times Reporter. (2015, December 09). Holiday makers: Watch out for cyber bullies. Retrieved from The New Times: <https://www.newtimes.co.rw/section/read/195119>
- Tustin, D. H., Zulu, G. N., & Basson, A. (2014). Bullying among secondary school learners in South Africa with specific emphasis on cyber bullying. *Child Abuse Research: A South African Journal*, 15(2), 13-25.
- UK Government. (April 2019). Online Harms. London: APS Group on behalf of the Controller of Her Majesty's Stationery Office. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf
- UNFPA. (2008). Country Assessment on Violence Against Women, Rwanda. United Nations Population Funds. Retrieved from http://www.un.org/womenwatch/ianwge/taskforces/vaw/VAW_COUNTRY_ASSESSMENT-Rwanda-1.pdf
- UNICEF Rwanda. (2017). Children's rights and sustainable development in Rwanda: A situation analysis. UNICEF. Retrieved from http://files.unicef.org/transparency/documents/Rwanda_SitAn_FullReport_2017.pdf
- World Economic Forum. (2016). The Global Gender Gap Report 2016. Geneva: World Economic Forum. Retrieved from http://www3.weforum.org/docs/GGGR16/WEF_Global_Gender_Gap_Report_2016.pdf
- Zulu, G., & Tustin, D. H. (2012). Nature, extent and impact of bullying among secondary school learners in Gauteng. Presentation at Gauteng Department of Education 5TH Monitoring and Evaluation Colloquium. Retrieved from <http://www.gauteng.gov.za/government/departments/education/Specialised%20Documents/Bureau%20of%20Market%20Research.pdf>

For generations we have in culture, in our national laws and by international agreement, supported children on their journey from dependence to autonomy across all aspects of society. This reflects our understanding that the capacity of a child to act in their own best interests is necessarily limited by vulnerabilities and immaturities associated with their age which means that the young require special privileges and care.

The digital environment must reflect this consensus.

1/3rd of those online are under 18, which amounts to nearly one billion children. 5Rights Foundation works towards a digital environment that anticipates the presence, meets the needs and upholds the rights of children.