Cyber-Safety Policy Elements in the Era of Online Learning: A Content Analysis of Policies in the UAE

Nur Siyam¹ · Malak Hussain¹

Accepted: 12 February 2021 / Published online: 22 February 2021
© Association for Educational Communications & Technology 2021

Abstract

With the increased level of technology usage in schools and the move to online learning, many schools had to re-evaluate the content of their cyber-safety policy and review it to ensure it works within and beyond the schools' premises. This study aimed to analyse the cyber-safety policies of twenty private schools in Dubai, an emirate in the United Arab Emirates (UAE). Five main categories were considered for the content analysis of the policy documents including definitions, preventive measures, reporting and responding to incidents, connection to other policies and mention of existing legislation. Upon the analysis of the policy documents, it was found that while some addressed cyber-safety issues, the focus remained more on cyberbullying incidents. Besides, the development of the cyber-safety policies is lacking the input from the concerned authorities whose ultimate responsibility is to develop the major policies and guidelines to be adopted by schools.

Keywords Cyber-safety · Cyberbullying · Policy · Education

Introduction

Technology has introduced a new set of social and behavioural risks, where the youth are found to be the most vulnerable (Von Solms and Von Solms 2015). Parents tried to set rules and protocols. However, taking into consideration the wide gap of technology literacy between the parents and their kids, parents were unable to ensure full authority to eliminate risks. Here came the role of schools in educating the children on safe online behaviour through well-defined policies (Von Solms and Von Solms 2015).

Bullying, which can be defined as a “systematic abuse of power” (Sharp and Smith 2002, p. 2), has been the interest of research since the late 70's. However, the technology invasion, especially with the appearance of the second generation of digital network phone in the 1990s, has introduced a new evolving form of bullying, called cyberbullying (Donegan 2012).

Recently, the unprecedented circumstances of Covid-19 pandemic, that hit the world during the academic year 2019–

2020, necessitated the closure of schools around the world, including in the United Arab Emirates (UAE), and the complete shift to distance e-learning. Students became obliged to be always online using various applications including social media platforms to complete their work and interact with teachers and classmates (Gupta and Jawanda 2020; Tas'adi et al. 2020).

According to many studies, the risks of being exposed to cybercrimes have increased due to the Covid-19 pandemic (Jain et al. 2020; Medina et al. 2020). Therefore, the urgency of having well defined policies to protect the children has increased as well (Kozma and Isaacs 2011; Redmond et al. 2020). Consequently, educational authorities and institutions had to re-think their e-safety guidelines and re-study their current national curricula and policies. In the UAE, for instance, new guidelines have been formulated and issued along with the start of the distance learning (DL) initiative due to the pandemic (UAE Ministry of Education, 2020). These guidelines aimed to promote positive and responsible behaviour among students, ensure the success of the DL initiative by creating an appropriate educational environment, reduce behavioural offenses outside the school's physical boundaries, and provide a reference for rules, standards and procedures that deal with problematic students behaviour, including cyber-bullying and technical offenses.

✉ Nur Siyam
nur.siyam@gmail.com

¹ The British University in Dubai, Dubai, UAE

However, there were no implications that these will be integrated into the national curricula. Furthermore, the Ministry of Education in the UAE oversees the public education sector in the UAE whereas the private education sector in the emirate of Dubai is overseen by The Knowledge and Human Development Authority (Knowledge and Human Development Authority 2020a) and the private education sector in Abu Dhabi is overseen by the Abu Dhabi Department of Education and Knowledge (ADEK) (ADEK 2020). Therefore, the proposed framework by the Ministry of Education did not apply to private schools in Dubai. That being so, the lack of clear guidelines for private schools in Dubai regarding cyber-safety policies has motivated this study, especially after the pandemic forced schools to move online, which resulted in an increased rate of cybercrimes and cyberbullying incidents (Tabrez 2020). The need to ensure that children's safety and wellbeing policies apply within and beyond the school's boundaries influenced the need to investigate the elements of a comprehensive cyber-safety policy that will ensure students are protected regardless of their mode or place of study.

This research aimed to identify the essential elements of a cyber-safety policy document in general and to examine the content of the cyber-safety policy documents of a sample of private schools in Dubai against the criteria that the literature suggests. Thus, this paper aimed to answer the following questions:

- What are the essential elements of a Cyber-Safety policy document?
- What are the evident elements and components in different Cyber-Safety policy documents in Dubai?

It is worth mentioning that this study was conducted during the academic year of 2019–2020, when schools in Dubai were operating fully online for one month. Thus, the policy documents evaluated may not have been amended to accommodate the new challenges or were not specifically developed for distance learning.

Literature Review

Cyber-Safety

Cyber-Safety or Cyber-Security refers to the safe and desirable practices in online environments which include being responsible when using online information and outlets. It also includes the specific procedures that are followed in case of improper and unsafe use of these technologies (Shamsi 2019). Cyber-safety practices in the school context aim to ensure the safety and well-being of students when working online and to prevent the occurrence of cybercrimes or risks. Cybercrimes

are defined as any type of illegal activities that are conducted via digital means. This includes, but is not limited to, phishing, data and identity theft, infection of systems by malware (i.e., viruses), cyber sexual predation, exposure to inappropriate content, and cyberbullying (Richardson et al. 2020).

Cyberbullying

Cyberbullying, while not the only form of cybercrimes, has been the focus of many school policies for its high prevalence rate between students, specially pre-teens and teens (Brown et al. 2006). Cyberbullying, in a school context, mainly involves unethical and aggressive behaviour where groups or individuals harass and hurt other students or staff in a deliberate and repeated manner. Examples include, but are not restricted to, the following: intimidating messages or emails, online abuse or scorn, offenses and insults, derogatory websites, circulation of private pictures/videos, fake profiles, and impersonation (Foody et al. 2017a). Both cyberbullying and conventional bullying can result in detrimental effects on the victims both on the personal and social level. Conventional bullying, however, can be handled much easier and measures can be escalated to ensure full stop of such behaviour, due to taking place inside the school walls and the limited number of involved people. Cyberbullying, however, which can occur inside the school too, is usually more frequent outside school hours (Brown et al. 2017).

Cybercrimes in general, and cyberbullying in specific, are considered challenging behaviours as they occur online and can be hard to track, identify or prevent. However, it remains the school's responsibility to establish measures to prevent and act upon cybercrimes considering that at least the victim is a student in the school (Foody et al. 2017a; Thomas 2010).

Cyber-Safety Policies

Policies and procedures are forged to govern all facets of school operations and to impact all decisions and practices to ensure transparency and effectiveness (Brown et al. 2017; Chalmers et al. 2016). Although there is no agreement upon a one-size-fits-all method for preventing cybercrimes (and the cyber-risks resulting from them) in schools, numerous global responses to the issue have been proposed (Ryan 2017). For instance, the Cooperation of Science and Technology (COST) synthesized fifty-four guidelines from twenty-seven European countries with the aim of sharing expertise on cyberbullying in schools and moving towards a common framework applicable in Europe (Välimäki et al. 2012). Recommendations for schools included the need for all school members to have access to clear information and support for preventing, detecting, reporting, and responding to cyberbullying incidents.

The government of the UAE considered the safety of its citizens in general and that of its children in specific.

Stemming from this and to attend to the alarming consequences that are resulting from the long time that children spend in front of their devices playing online games or using their mobiles for social media or even doing their schoolwork, the UAE has initiated cyber security awareness programs for children to educate them about safe internet use (Al Shamsi 2019). One of these programs is the “Child Digital Safety” initiative, which is a joint program between the Ministry of Interior and the National Happiness Program launched on the Emirati children’s day on March 15 in 2016. This initiative is one of a series of programs aiming to raise digitally literate generations (UAE Ministry of Cabinet Affairs, 2019).

The Abu Dhabi Department of Education and Knowledge (ADEK) (ADEK 2020), the legislative authority for the private schools in Abu Dhabi, has issued in 2015 the private school’s policy guidance manual that included policies that aimed at building a sustainable private education system that is able to self-improve, has good governance, and exhibits matured operational capabilities. Among the policies included in the manual is the “Protection from Dangers of the Global Information Network (the Internet)” policy. This policy aims to protect students from offensive or inappropriate online content, educate students on online ethics and safety, and promote good online practices (Abu Dhabi Department of Education and Knowledge 2015).

In response to the Covid-19 pandemic that resulted in schools in the UAE to shift fully to distance learning, the Ministry of Education in the UAE, has formulated new guidelines that aim to promote positive and responsible behaviour among students and ensure the success of the DL initiative (UAE Ministry of Education, 2020). The guidelines include procedures for dealing with online offences and outlining the roles and responsibilities of all schools’ community members.

The Knowledge and Human Development Authority (KHDA) is the regulatory authority and the educational quality assurance regulator of the Government of Dubai, whose role is to ensure that Dubai private schools are operating in line with its legislation and according to the highest quality standards. The KHDA has dedicated one performance standard in its inspection framework for schools for “Protection, Care, Guidance, and Support of Students. One of the elements of this standard is “Care, welfare and safeguarding of students, including child protection”. The descriptors of this standard appraise a school based on the availability (or lack of thereof) of rigorous safeguarding procedures of students including child protection. This standard measures whether all stakeholders are fully aware of these procedures, and whether the school is highly effective in protecting students from all forms of abuse, among which is cyberbullying. The school will be rated “very weak” if it does not conform to clear procedures for safeguarding (Knowledge and Human Development Authority 2015). However, the KHDA, as the legislative authority for private schools in Dubai, has not developed nor

published clear guidelines for safeguarding and child protection that would serve as a reference for all private schools and from which they can develop their own policies.

Most recently, a smart security structure “Aqdar e-Safe Schools” was launched in the public and private schools in the UAE (e-Safe School 2020). The initiative, which follows the European Union standards for e-safety in education, aimed to help schools create and review their online safety policies and practices through guided steps.

Despite the various international, national, and local initiatives aiming to address cyber-safety in general and cyberbullying in particular, they both remain an area of concern that requires further investigation and attention both locally and internationally. Schools might have established anti-bullying policies and guidelines, but efforts need to be assimilated to ensure implementation is more effective (Chalmers et al. 2016).

Related Work

For a policy to achieve the desired outcomes as per the set plan of action, it must be concise and unambiguous. A comprehensive cyber-safety policy should include effective procedures and practices that would help prevent cybercrimes in the first place, and deal with it if it happens in the second place according to comprehensive intervention strategies (Chalmers et al. 2016; Foody et al. 2018).

In many countries where more extensive research has been conducted on policy development, such as the United Kingdom and the United states of America, it is a legal obligation for schools to have an anti-bullying policy (Chalmers et al. 2016). In such countries, governments and educational organizations provide districts and schools with policy frameworks that aim to provide clear guidelines for policy makers. Thus, most of the schools in such countries have separate anti-bullying policies rather than having it as a part of a behaviour and discipline policy (Foody et al. 2017b).

Previous work aimed to evaluate the effectiveness of cyber-safety policies to provide guidance for policymakers and schools. For instance, the Working Group 3 of COST Action IS0801 produced a booklet to address cyber-bullying by examining fifty-four guidelines from twenty-seven European countries (Välimäki et al. 2012). This work aimed to carry out a content analysis to identify the strengths and weaknesses of the examined guidelines to point out elements of good practice. The guidelines were examined from four distinct points of views according to targeted groups including parents, children, schools, and teachers. Results from the analysis indicated that many guidelines mentioned the role of parents, the importance of developing awareness among students to help them recognize and report cyberbullying, the importance of developing online skills for young children, and the role of teachers in helping students develop the needed skills

and awareness. However, fewer guidelines mentioned the importance of collaboration between parents and schools, outlined the steps to be taken to report cyberbullying incidents, or outlined the role of teachers in creating and evaluating policies as well as in developing their own skills. Moreover, most of the guidelines were lacking the input from the concerned authorities whose ultimate responsibility is to develop the major policies and guidelines to be adopted by schools (Brown et al. 2017; Chalmers et al. 2016).

Brown et al. (2006) reviewed existing research on cyberbullying to provide recommendations for a policy framework. The authors argue that at the school level, there is a need for acceptable use policies that expand to include online behaviour inside and outside the school. The authors also affirmed that students should have a role in developing relevant policies. The authors also emphasized on the need to critically evaluate the effectiveness of policies to determine if they are succeeding in reducing cyber-crimes and cyberbullying incidents. More recently, Redmond et al. (2020) developed a cyberbullying conceptual framework for educators. In their work, the authors reviewed the literature on cyberbullying in schools to identify common terms. The study resulted in the development of a framework that consists of three main categories: identification, managements, and prevention. For the identification category, four elements were identified: understanding the attributes of cyberbullying, knowledge of the types of cyberbullying, identifying student awareness of cyberbullying, and educators' perspectives of cyberbullying. For the management category, two elements were identified: the role and responsibility of the school and that of the educator. Finally, for the prevention category, three elements were identified: the role and responsibility of the school, the teacher, and the teacher education program.

Foody et al. (2017a) evaluated legislative and public policy solutions to cyberbullying available in Qatar. The authors pointed out that there is an absence of guidelines withing the current legislation for schools for dealing with cyberbullying incidents as well as statistics on the number of schools that have anti cyberbullying policies. And while there is a behavioural policy developed by the Supreme Education Council, the policy is considered lacking. The authors reported that the behavioural policy includes definitions of bullying and cyberbullying and a list of preventative measures. However, the policy does not include the role of parents and students and the follow-up measures. Moreover, there is no research investigating the impact of this policy on bullying and cyberbullying rates in Qatar. The authors emphasized on the need for schools to have a comprehensive procedure to follow when cyberbullying incidents occur. The authors maintained that schools should be legally required to have cyberbullying policies that outline the roles and responsibilities of all concerned parties as well as clear procedures to follow when an incident is reported. Additionally, the authors mentioned the

need to record and document cyberbullying incidents as well as the need to provide support for victims and bullies.

Chalmers et al. (2016) examined anti-bullying policy development in three states in Australia. All schools in Australia are required to adhere to the National Safe Schools Framework (NSSF) guiding principles when developing their policies. Research has found that the implementation of the NSSF framework resulted in declined rates of self-reported bullying incidents. It was also reported that greater support is needed to ensure teachers uptake the recommended practices. The study found that the definition of cyberbullying differs from one policy framework to another. Additionally, most of the definitions did not correspond fully to the commonly agreed definition of bullying by researchers, which includes a repetition of behaviour, with the intention to cause harm and with an imbalance of power (Olweus 2000). Additionally, the study found that some specialists believed that cyberbullying requires a unique policy separate from the bullying policy, as the later was developed before the emerging of cyberbullying. Regarding the elements of a cyberbullying policy, the study found that to be effective, the policy should be clear and consistent, and should include clear definitions of all forms of cyberbullying, preventive and educative measures, procedures for interventions, consequences, accepted behaviour for students, specific roles, and procedures for reporting incidents to school authorities. However, the authors noted that gauging the effectiveness of cyberbullying policies on reducing bullying behaviour is understudied.

Considering the importance of having a national cyber security policy framework that informs policies in schools, de Lange and von Solms (2012) aimed to propose a framework that can be used to promote a cyber-safety culture in South African schools. The authors proposed a framework that incorporates five criteria: governance (i.e., e-safety policy), role players (i.e., school, teachers, parents, and students), topics (i.e., education), resources (i.e., internal, and external), and delivery (i.e., curriculum and communication).

In another study in South Africa, Kritzinger (2016) also indicated that there is little support from education authorities to deal with the issue of cyberbullying. The study noted that only the minority of schools received training on cyber-safety practices. It also indicated that only half of the schools had a formal cyberbullying policy in place. Only few schools outlined in their policies specific guidelines on cyberbullying or information about integrating cyber-safety in the curriculum. Conversely, most of the policy documents focused on ensuring access restrictions are in place, such as restrictions to mobile, internet, and social media access.

Cyber-safety policies have also been the focus of many national and international organizations. For instance, the Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Centre developed a

document for cyber-safety considerations in the United States of America (Readiness and Emergency Management for Schools 2017). The document suggests that schools should create responsible use policies that include information about appropriate online behaviour, the use of filtering and blocking software to prevent access to inappropriate content, education about online risks and how to stay safe, and procedures to prevent and act upon cybercrimes incidents.

Previous studies conducted content analysis of anti-bullying policies. In their two studies on anti-bullying policies in England, Smith et al. (2012, 2008) devised a scoring scheme to assess policies. In the first study (Smith et al. 2008), the authors found that most policies included definitions of bullying with reference to its different forms and a statement on how parents will be informed when incidents of bullying occur. However, few schools included mentions of responsibilities of those other than the teachers, following up incidents, record keeping, and preventative measures. In their follow up study (Smith et al. 2012), the authors noted several improvements in policies. However, still missing from most of the policy documents were specific forms of bullying, such as cyberbullying and teacher-student bullying as well as special preventative measures, such as peer support.

Having a cyber-safety policy implies the school's commitment to cyber-safety and anti-bullying work. This includes preventative and corrective strategies, as well as communicating these strategies to the school's community. However, previous research indicates that the content and quality of school policies varies widely, questioning their effectiveness in reducing cyberbullying and cyberattacks incidents (Smith et al. 2008). Moreover, there is a lack of analysis of current cyberbullying and cyber-safety policies. While having a policy in place is essential, it should be clear and comprehensive to be properly used by stakeholders and be effective (McNeal et al. 2016).

Despite the wealth of international research, cyberbullying in schools is relatively under-studied in the UAE (AL Nuaimi 2021). However, there has been renewed interest in recent years, including studies that tackled the issue of cyber security in schools by evaluating the effectiveness of cyber security programs (Shamsi 2019), exploring cyberbullying in social media among university students (Abaido 2020), and studying the characteristics of cyberbullying and cyberstalking laws in the UAE (Hosani et al. 2019).

Methodology

In this research, the cyber-safety policy documents of twenty private schools in Dubai have been analysed against the main components of a cyber-safety policy according to literature.

Data Collection

A search was performed using a combination of the keywords “Cyber-Safety”, “Cybersecurity”, “Cyberbullying”, “School Policy”, and “Dubai” to find private schools in Dubai that have a specific cyber-safety policy plan. General child safety policies were not selected. Anti-bullying policies without a specific section for cyberbullying were not selected as well. A total of twenty policy plans for twenty schools were selected for this study. Four of the schools followed an American curriculum. Four of the schools followed an Indian curriculum. The remaining sixteen schools followed a UK curriculum. All the schools were k-12 schools. There are 169 private schools in Dubai catering to over 89% of the student population in the emirate (Knowledge and Human Development Authority 2020b). The sample of policy documents retrieved was limited to the public availability of the document.

Procedures

A content analysis was designed for the cyber-safety policies. The list was devised considering the essential components of a cyber-safety policy according to the reviewed literature as well as available policy guidance frameworks from international and national associations (see Table 1). The initial list was piloted with 5 policies and some minor modifications were made before the list was finalized. The list was divided into five main categories with a total of 22 element. The five categories were: (A) Definitions (4 elements), (B) preventive measures (5 elements), (C) reporting and responding to incidents (7 elements), (D) connection to other policies (4 elements), and (E) mention of exiting legislation (2 elements). For each element, the school either scored one or zero for meeting the criteria or not meeting it, respectively. As shown in Table 2, each section was subtotalled. Moreover, a total overall cyber-safety policy content score was produced.

Cyber-Safety Policy Elements

In this section, we describe the elements of a cyber-safety policy which the policy documents of the schools are analysed against. The elements are based on previous research on cyber-safety (Chalmers et al. 2016; de Lange and von Solms 2012; Foody et al. 2017a; Marczak and Coyne 2010; Redmond et al. 2020; Shamsi 2019), cyber-safety national and local policies (Abu Dhabi Department of Education and Knowledge 2015; Independent Education Union 2011; Readiness and Emergency Management for Schools 2017; UAE Ministry of Education, 2020; Välimäki et al. 2012), and other research examining the content of similar policies (such as bullying and cyberbullying policies) (Smith et al. 2012; Smith et al. 2008). Moreover, the categories are based on the cyberbullying framework for educators proposed by

Table 1 Devised list for the components of a cyber-safety policy

	Categories/Elements	Description	Reference
A	Definitions (4 items)		
1	Includes Cyber-Safety definition	The definition includes the protection of the user and its assets from any online threats through various measures such as promoting cyber safe behaviours as well as management measures.	(Independent Education Union 2011; Redmond et al. 2020)
2	Includes Cyberbullying definition	The definition includes the repetition of an action and the intention to cause harm.	(Chalmers et al. 2016; Independent Education Union 2011; Redmond et al. 2020; Smith et al. 2012)
3	Includes a list of cyber-risks forms	Includes, but is not limited to, phishing, data and identity theft, infection of systems by malware, cyber sexual predation, exposure to inappropriate content, and cyberbullying.	(Independent Education Union 2011; Redmond et al. 2020; Smith et al. 2012)
4	Includes a list of cyberbullying forms	Includes, but is not limited to, exclusion or peer rejection, harassment, or ‘cyberstalking’, outing, impersonation and fake profiles.	(Independent Education Union 2011; Redmond et al. 2020; Smith et al. 2012)
B	Preventive Measures (5 items)		
1	Mentions policy relation to curriculum	Mentions the integration of cyber-safety education into existing or special units of study.	(Chalmers et al. 2016; de Lange and von Solms 2012; Independent Education Union 2011; Marczak and Coyne 2010; Readiness and Emergency Management for Schools 2017; Shamsi 2019)
2	Mentions policy relation to schools’ activities (i.e., assemblies, bulletins)	Mentions the preventative role of cyber-safety promotion through means outside the curriculum such as morning assemblies, magazines, and drama presentations.	(de Lange and von Solms 2012; Independent Education Union 2011)
3	Mentions Professional Development or training for Staff	Discusses if or how teachers will receive professional development about their rights and responsibilities, how and when to apply the policy, and how they are expected to deliver the education programs related to the policy. (“professional development for teachers” is sufficient if it clearly refers to cyber-safety training)	(Chalmers et al. 2016; Foody et al. 2017a; Independent Education Union 2011; Readiness and Emergency Management for Schools 2017)
4	Mentions communicating updates with stakeholders	Discusses how the schools will continuously communicate updates regarding what is expected and acceptable to all stakeholders (teachers, parents, students).	(de Lange and von Solms 2012; Independent Education Union 2011)
5	States students code of conduct regarding cyber-safety inside the school	Mentions how students are expected to behave online. This includes cyber-safety practices such as password security, as well as accepted online behaviour.	(Foody et al. 2017a; Independent Education Union 2011; Readiness and Emergency Management for Schools 2017)
C	Reporting and Responding to incidents (7 items)		(Chalmers et al. 2016)
1	Mention of the extent of the school concerns of incidents happening outside the school’s hours	Clarifies that the policy applies to all cyber-security issues, including those happening outside the school physical boundaries.	(Brown et al. 2006; Foody et al. 2017a; Smith et al. 2012)
2	States what victims or witnesses of cyberattacks and cyberbullying should do	E.g., report to a teacher	(Chalmers et al. 2016; Foody et al. 2017a; Independent Education Union 2011; Marczak and Coyne 2010; Smith et al. 2012)
3	States how teaching staff should respond to a report of cyberbullying or cyberattack	More specific than just “deal promptly”.	(Independent Education Union 2011; Smith et al. 2012)
4	States how parents should respond and report a cyberattack	E.g., save any offending material and contact the students’ counsellor.	(Foody et al. 2017a; Smith et al. 2012)
5	Mentions how incidents will be handled and followed up	Include the procedures that will be implemented in different situations and according to the intensity of the offense and how the incident will be followed up.	(Chalmers et al. 2016; Foody et al. 2017a; Smith et al. 2012)

Table 1 (continued)

	Categories/Elements	Description	Reference
6	Mentions procedures to maintain logs.	States that report of incidents will be recorded.	(Foody et al. 2017a; Independent Education Union 2011; Marczak and Coyne 2010; Smith et al. 2012)
7	Mentions how or if victims will be supported	States that victims will be supported.	(Foody et al. 2017a; Smith et al. 2012)
D	Connection to other policies (4 items)		
1	Refers to electronic device usage agreement	Demonstrate links, or includes electronic device usage agreement or policies.	(Independent Education Union 2011)
2	Refers to discipline and behaviour policies	Demonstrate links to existing school's behaviour or discipline policies.	(Independent Education Union 2011)
3	Refers to anti-bullying policy	Demonstrates links, or includes traditional anti-bullying policies.	(Independent Education Union 2011)
4	Refers to safeguarding and child-protection policy	Demonstrates links to safeguarding and child-protection policies.	(Independent Education Union 2011)
E	Mention of Existing Legislation (2 items)		
1	Refers to cyber laws	Refers, at least implicitly, to any of the UAE Cyber Crimes Laws (2012, Available at: https://u.ae/en/resources/laws ; 2016) (UAE Government 2020)	(Independent Education Union 2011)
2	Refers to Privacy/Digital Content Laws	Refers, at least implicitly, to the UAE Internet Access Management regulatory policy (2017) (UAE Government 2020)	(Independent Education Union 2011)

Redmond et al. (2020) as well as the categories and elements proposed by Smith et al. (2012, 2008). The main categories of the policy should include definitions, preventive measures, and procedures for managing incidents. In addition to these categories, we add one more dimension that includes the connection of the cyber-safety policy with other school's policies and local laws and legislations (Independent Education Union 2011).

The first category examined is “definitions”. Including definitions in a policy document facilitates the understanding of the policy and the identification of issues in order to meet the intention of the document (Kusserow 2008). We examine four items under the “definitions” category: cyber-safety definition, cyberbullying definition, cyber-risks forms, and cyberbullying forms. Cyber-safety definition should include the mention of measures to promote cyber safe behaviours based on the safe, respectful and responsible use of the internet and technology devices, in addition to the measures taken to remove the risks of such use (Independent Education Union 2011). The mention of cyber-risks forms allows the audience of the policy to understand how the policy extends beyond cyberbullying, covering issues such as phishing, data and identity theft, infection of systems by malware (i.e., viruses), cyber sexual predation, exposure to inappropriate content, and cyberbullying (Richardson et al. 2020). The definition of cyberbullying resembles the definition of bullying except that it uses electronic media. Unlike

bullying, cyberbullying does not consider the power imbalance component, as technology can enhance the perpetrator power (Redmond et al. 2020). The definition should include the repetition of an action and the intention to cause harm (Smith et al. 2012). Cyberbullying forms include, but are not limited to, exclusion or peer rejection, harassment or ‘cyberstalking’, outing (i.e., circulation of private information or images), impersonation and fake profiles (Independent Education Union 2011; Redmond et al. 2020).

The second category encompasses preventive measures. To ensure effectiveness of cyber-safety policies, they should be associated with cyber-safety education and promotion of positive uses of technology throughout the school community (de Lange and von Solms 2012). Many studies indicated that bullying can be reduced through structured curricula (Redmond et al. 2020). One common way for schools to promote cyber-safety awareness is by teaching digital citizenship. Responsible digital citizenship includes topics such as internet etiquette and internet safety (Redmond et al. 2020). Cyber-safety should be also promoted outside the classroom. This can include educating and informing students through drama presentations, morning assemblies, magazines and bulletin boards (Independent Education Union 2011). The policy should also detail how other members of the school's community, such as teachers and parents, will be educated (de Lange and von Solms 2012). It has been argued that successful prevention and management of

Table 2 Mean scores and Standard Deviation (SD) for each category (A. B. C, D and E), and for total cyber-safety content, and for each of the 22 elements as percentages

A	Definitions (4 items)	Mean=1.55 SD=0.94
1	Includes Cyber-Safety definition	20%
2	Includes Cyberbullying definition	25%
3	Includes a list of cyber-risks forms	20%
4	Includes a list of cyberbullying forms	90%
B	Preventive Measures (5 items)	Mean=2.8 SD=1.51
1	Mentions policy relation to curriculum	75%
2	Mentions policy relation to schools' activities (e.g., assemblies, bulletins)	70%
3	Mentions Professional Development or training for Staff	35%
4	Mentions communicating updates with stakeholders	30%
5	States students code of conduct regarding cyber-safety inside the school	70%
C	Reporting and Responding to incidents (7 items)	Mean=5.15 SD=1.14
1	Mention of the extent of the school concerns of incidents happening outside the school's hours	50%
2	States what victims or witnesses of cyberattacks and cyberbullying should do	90%
3	States how teaching staff should respond to a report of cyberbullying or cyberattack	80%
4	States how parents should respond and report a cyberattack	85%
5	Mentions how incidents will be handled and followed up	25%
6	Mentions procedures to maintain logs.	40%
7	Mentions how or if victims will be supported	80%
D	Connection to other policies (4 items)	Mean=2.3 SD=1.22
1	Refers to electronic device usage agreement	50%
2	Refers to discipline and behaviour policies	60%
3	Refers to anti-bullying policy	70%
4	Refers to safeguarding and child-protection policy	50%
E	Mention of Existing Legislation (2 items)	Mean=0.8 SD=0.77
1	Refers to cyber laws	60%
2	Refers to Privacy/Digital Content Laws	20%
Total 22 item		Mean=12.6 SD=2.50

cybercrimes, including cyberbullying, lies in the teacher continued education. Therefore, the policy should include if and how teachers will be trained. Additionally, cyberbullying can occur when students are at home with parents that may be unaware of what their children are doing online. Therefore, the mention of how parents will be educated is an essential part of the cyber-safety policy (Redmond et al. 2020). The ultimate goal of cyber policies that are implemented in schools is to protect children from online risks and harassment by ensuring that they are aware of acceptable online behaviour, the potential risks, and how to deal with them. Thus, an effective cyber-safety policy that would allow the school to fulfil its responsibilities in protecting its students would include a clear code of

conduct, including the school's expectation of students' positive behaviour, and how they deal with others (Chalmers et al. 2016).

The third category in a cyber-safety policy includes how incidents will be reported, managed, and documented. What is unique about cyber policies is that they expand outside the school's physical boundaries (Chalmers et al. 2016). While cybercrimes still occur inside the school, they are usually more frequent outside school hours (Brown et al. 2017). Thus, cyber-safety policies should clearly clarify that the policy applies to all cyber-security issues considering the victim is a student in the school (Foody et al. 2017a; Thomas 2010). Moreover, the policy aim should be clearly stated that would

elicit the corresponding roles and responsibilities of all stakeholders, including students, teachers, and parents as well as a clear reporting mechanism. The policy would also include the procedures that will be implemented in different situations and according to the intensity of the offense and how the incident will be followed up (Chalmers et al. 2016; Independent Education Union 2011). Additionally, mentions on how incidents logs will be maintained would be part of an effective policy. As with traditional bullying, policy documents would also include suggestions on how, or if, the victims will be supported (Smith et al. 2008).

Finally, it is also suggested that policies include summaries and/or links to existing related school policies and procedures like discipline, anti-bullying, child protection, school-wide discipline plan, and other ICT policies (Independent Education Union 2011). Schools are also encouraged when initiating any initiative that incorporates technology or ICT, to have integrated within the specific policy, a document entitled such as “Parent/Student Contract” or “Code of Conduct” or “Acceptable Use Policy”. Both the parent and the student will have to sign the document before they are granted the permission to access the internet through the school’s or their personal electronic device, to acknowledge that they have read through and that they agree with the terms, guidelines or the standards that are laid out in the policy and agreement and they hold full responsibility of the consequences in case of misuse (Readiness and Emergency Management for Schools 2017). Links to related national and international legislations, when included in the policy document, will make it more solid and more effective (Foody et al. 2017a). The UAE is considered to have the most detailed cybercrime laws in the Middle East (Hosani et al. 2019). The Federal Law No.1 (Cyber Crimes Law 2006, Available at: <http://www.ejustice.gov.ae>) considers it an offence to use of the internet or other technological tools to threaten individuals. The UAE-Law No. 5 (Cyber Crimes Law 2012, Available at: <https://u.ae/en/resources/law>) is concerned in general computer crimes such as fraud, unauthorized access, data breach, and other crimes against State security (Hosani et al. 2019). Additionally, Law No. 2 (Cyber Crimes Law 2015, Available at: <https://www.moj.gov.ae/en/laws-and-legislation/latest-legislations-and-laws.aspx>) addresses slander, defamation, discrimination, hatred, and threats which are forms of cyberbullying. Consequently, threats of violence, invasion of privacy, and damaging someone’s reputation are considered a form of cyberbullying and stalking, which are against the law in the UAE (Hosani et al. 2019).

Findings

Score Reliability

All the policies were scored by both researchers independently. There was a 100% agreement in 19 elements, and 90%

agreement in 3 elements. The disagreement occurred for the two items referring to existing legislation, as whether to consider this element present even if the law was not explicitly mentioned (i.e., UAE Digital Content Law). For example, a policy document may refer to the law implicitly; “*It can be an illegal act as in the UAE it is unlawful to disseminate defamatory information in any media*”. The authors agreed to consider the implicit mention of the law as referring to the law (item E1). The same was considered true for item E2. For item C7, one of the authors considered mentions of support as an evidence of the element presence (e.g., “*The school supports both the victim and the bully, as appropriate.*”) while the other author required the kind of support students will receive to be clearly stated. Thus, the wording of the element was changed to include the mention of the support, even if the details were not illustrated, as many schools consider this as part of the safeguarding and child-support policies.

Analysis

The total cyber-safety content scores ranged from 9 to 18, with a mean of 12.6 (63%) and a standard deviation of 2.50. That is to say, policy documents that were scanned contained 12.6 elements out of 22 in average, with documents containing as low as 9 elements and as high as 18.

For category A, scores ranged from 0 to 4 (out of 4), with a mean of 1.55 (38.9%). For category B, scores ranged from 1 to 5 (out of 5), with a mean of 2.8 (56%). For category C, scores ranged from 3 to 7 (out of 7), with a mean score of 5.15 (73.5%). For category D, scores ranged from 0 to 4 (out of 4), with a mean score of 2.3 (57.5%). Lastly, for category E, scores ranged from 0 to 2 (out of 2), with a mean of 0.8 (40%).

Table 2 shows the percentage for each element for policy documents that scored for the presence of this element. Elements that scored at or above 70% were considered as having high presence, while elements scoring at or under 30% were considered as low. Elements that scored between 30% and 70% were considered moderate.

For category A, including a list of cyberbullying forms scored high, while including a definition for cyber-safety and cyberbullying and the forms of cyber-risks had a low score. For category B, mentions of the policy relation to the curriculum and school’s activities as well as the code of conduct had a high score, while mentions of professional development or training for staff on cyber-safety had a moderate score. Conversely, mentions on how updates will be communicated with stakeholders had a low score. For category C, all elements corresponding to the reporting mechanism scored high. Mentions of the school’s involvement in cyber-incidents happening outside the school’s hours and mentions of maintaining logs of incidents had a moderate score, while mentions of how incidents will be managed and followed-up had a low score. For category D, reference to anti-bullying

policies had a high score, while mentions of other policies (safeguarding, conduct, and electronic devices usage) had a moderate score. For category E, referring to cyber laws had a moderate score while referring to privacy or digital content forms had a low score.

Discussion

While the policies analysed were intended to be cyber-safety policies, the focus was mainly on cyberbullying. This could be attributed to the frequency of such incidents compared to other cyber-safety issues, in addition to the higher risk of cyberbullying on the school community (Brown et al. 2017). However, cyber-risks could be as critical and dangerous as cyberbullying, including sexting, phishing scams, and privacy breaches. Moreover, the unsupervised online presence of students online may result in a digital footprint that puts them in higher risks of cyberbullying, as their data and pictures become available to the public. Thus, this is an important aspect that policies should not ignore. While all the examined policies included a definition of cyberbullying, the definitions were not consistent and did not all match the common definition in the literature. For instance, only few schools mentioned the elements of repetition and intention, which are essential to consider an offense as bullying.

A low percentage of schools mentioned existing national and international legislations. Since cyber-safety issues may result in legal consequences, cyber-safety and cyberbullying policies should be related to the authorities' laws. It might be also argued that the scope of the school's responsibility to intervene when cyberbullying occurs outside the physical school setting should be determined and well-defined (Brown et al. 2017).

One of the important elements of a cyber-safety policy is outlining proactive preventive measures. Many policy documents did not include any indication of how cyberbullying can be prevented. Few policy documents included a detailed account on how the school community should be educated regarding cyberbullying and other cyber-safety issues. Also, few policy documents mentioned the incorporation of cyber-safety education into the curriculum. The Ministry of Education in the UAE provides cyber security education within the curriculum of the public schools. However, it does not mandate the incorporation of cyber security education in the curriculum of private schools. Nevertheless, schools are encouraged to teach students digital citizenship including topics such as privacy and security, communication, cyberbullying, digital footprints, reputation, copyrights, and plagiarism (Armfield and Blocher 2019; Gretter and Yadav 2016). The prevention of cyberbullying incidents necessitates educating those concerned in raising awareness of cyberbullying. While some policy documents stated the need for teachers'

professional development and training as well as communicating updates to parents, they failed to specify the content, frequency, and responsible staff to carry out such training.

The reporting mechanisms were missing from many policy documents. They were also limited to broad definitions without clear logistics of how and who. Having a cyber-safety policy in place is not enough if not accompanied by clear reporting procedures. Such procedures and guidelines should be clearly communicated with students, families, and staff (Chalmers et al. 2016).

Links to ICT policies, especially "Acceptable Use policies" were missing in half of the surveyed documents. Schools should emphasize the need to have students sign an agreement before using the school's Wi-Fi or bringing and using their own devices. Links to the school's anti-bullying policies were evident. However, links to the discipline and behaviour policy as well as the safeguarding and child-protection policy were not evident in all the surveyed documents.

In some countries, such as the United Kingdom and the United States of America, it is a legal requirement for all schools to have anti-bullying policies in place to handle both bullying and cyberbullying incidents (Chalmers et al. 2016). The absence of these links in some of the policy documents surveyed may be attributed to the fact that these connections are not a legal requirement in the UAE. While KHDA encourages all schools to have a child protection policy in place, there are no clear requirements regarding the cyber-safety and cyberbullying policy connection to other policies.

Implications and Conclusions

In this research, we aimed to identify the main elements of a school's cyber-safety policy document. We also aimed to examine the content of the cyber-safety policy documents of a sample of private schools in the United Arab Emirates against the criteria identified. Five main categories with 22 elements were identified, including definitions, mention of existing legislation, preventive measures, reporting and responding to incidents, and connection to other policies. By analysing the policy documents and scoring them against the cyber-safety content list proposed, it was clear that there is a great range of scores. By looking at the results, it can be concluded that a typical cyber-safety policy document for a school in Dubai will have a clear list of cyberbullying forms, mention policy relation to curricular links and activities, state the code of conduct for students regarding cyber-safety and cyberbullying issues, clearly state the roles and responsibilities of students, teachers and parents in reporting incidents, mention victims will receive support from the school, and refer to the anti-bullying policy or is part of it. On the other hand, it is unlikely that it will include a cyber-safety definition and its associated risks, refer to existing legislations, mention how teachers and

parents will be educated in regards of cyber-safety issues, mention how the policy applies for incidents outside the school, mention how the school will follow up incidents and maintain logs, and refer to other policies, such as electronic device usage, behaviour, and safeguarding policies. These results have many implications for policy, practice, and research.

Cyber-risks, including cyberbullying, remain a challenge for schools as incidents are hard to trace, allow the participation of many individuals, and may occur outside school's hours (Brown et al. 2017). All these challenges require clear local guidelines for schools to aid them in managing incidents with their available resources and to provide boundaries and direction as to the scope of their responsibility.

Efforts should also be done to improve the quality of the policies developed by schools to ensure their effectiveness to achieve their desired outcomes. To this, it would be essential to provide stakeholders who develop and create these policies with necessary extensive training to learn how to base the frameworks and guidelines of their policies on evidence-based research besides ensuring that they, themselves, are well-informed of what cyber-risks are in general and cyberbullying in particular (Chalmers et al. 2016). It has been recommended that schools are given feedback on their policies by specialized entities, without compromising the school's ownership of the school's strategies (Smith et al. 2012). A national cyber-safety policy framework on which schools base their policies would be recommended, which would make it easier for the stakeholders to handle cyberbullying and ensure cyber-safety (Cilliers and Chinyamurindi 2020).

Data provided in this research give important insights into the strengths and weaknesses of many school's cyber-safety policies. Many policy documents have missing crucial areas, including coverage of cyber-safety issues, education of stakeholders beyond students, and clear strategies to follow up incidents. It is important for schools to focus while developing their cyber-safety policies on the educators and their role in the whole process and the extent of authority they have when they interfere to protect their students from cyber-risks and cyberbullying both within and outside the school premises (Brown et al. 2017). Schools should also be encouraged to give more attention to cyber-safety policies for its increasing importance. Schools should research best practices, engage all the community stakeholders in the policy development process, and continually assess their policies. Moreover, schools should ensure that their policies are linked and in agreement to avoid conflict and reduce redundancy.

While this study is a first attempt to analyses the content of cyber-safety policy documents in the UAE, it is limited in various aspects. First, it only reports on policies that were available to the public. This resulted in a low response rate (20 out of 169 policy documents). However, this limitation

can be also considered an insight for practice where schools should be encouraged to share their policies with the community to allow parents easy access, either before enrolling their kids in the school or after. This study cannot claim to represent schools over the UAE other than private schools in Dubai, as other schools follow different jurisdictions. Additionally, the cyber-safety content list, which policies were scored against, may had overlooked some crucial items, or included elements that did not contribute to the effectiveness of the policy in preventing cyber-risks or cyberbullying incidents. Moreover, we do not include the elements related to the “policy creation”, such as who is responsible of creating the policy and managing the workflow for revising and updating the policy (Kusserow 2008).

Future research should attempt to correlate the quality and coverage of a policy with the actual levels of cyber incidents (Brown et al. 2006; Hatzenbuehler et al. 2015). Another valid correlation that should be attempted is with stakeholders' perceptions on the quality of cyber-safety procedures in the schools (AL Nuaimi 2021; Kraft and Wang 2009; Shamsi 2019).

Declarations

Conflict of Interest There are no conflicts of interest.

Research Involving Human Participants and/or Animals There are no participants in this research.

Informed Consent There are no participants in this review of documents. Therefore, no informed consent was needed for this study.

References

- Abaido, G. M. (2020). Cyberbullying on social media platforms among university students in the United Arab Emirates. *International Journal of Adolescence and Youth*, 25, 407–420. <https://doi.org/10.1080/02673843.2019.1669059>.
- Abu Dhabi Department of Education and Knowledge, 2015. Private-Schools-Policy-and-Guidance-Manual.pdf [WWW Document]. URL <https://www.adek.gov.ae/-/media/Project/TAMM/ADEK/Downloads/Private-schools/Private-Schools-Policy-and-Guidance-Manual.pdf> (accessed 7.8.20).
- ADEK, 2020. ADEK: About us [WWW document]. Us. URL <https://www.adek.gov.ae/en/About/About-Us> (accessed 12.29.20).
- AL Nuaimi, A. (2021). Effectiveness of Cyberbullying prevention strategies in the UAE. In S. Fong, N. Dey, & A. Joshi (Eds.), *ICT analysis and applications, Lecture Notes in Networks and Systems* (pp. 731–739). Singapore: Springer. https://doi.org/10.1007/978-981-15-8354-4_72.
- Armfield, S. W. J., & Blocher, J. M. (2019). Global digital citizenship: Providing context. *TechTrends*, 63, 470–476. <https://doi.org/10.1007/s11528-019-00381-7>.
- Brown, C., Demaray, M.K., Tennant, J.E., Jenkins, L.N., 2017. Cyber victimization in high school: Measurement, overlap with face-to-face victimization, and associations with social-emotional

- outcomes. *Sch. Psychol. Rev.* 46, 288–303. <https://doi.org/10.17105/SPR-2016-0004.V46-3>.
- Brown, K., Jackson, M., Cassidy, W., 2006. Cyber-bullying: Developing policy to direct responses that are equitable and effective in addressing this special form of bullying. *Can. J. Educ. Adm. Policy*.
- Chalmers, C., Campbell, M. A., Spears, B. A., Butler, D., Cross, D., Slee, P., & Kift, S. (2016). School policies on bullying and cyberbullying: Perspectives across three Australian states. *Educational Research*, 58, 91–109. <https://doi.org/10.1080/00131881.2015.1129114>.
- Cilliers, L., & Chinyamurindi, W. (2020). Perceptions of cyber bullying in primary and secondary schools among student teachers in the eastern Cape Province of South Africa. *Electron. J. Inf. Syst. Dev. Ctries.*, 86, e12131. <https://doi.org/10.1002/isd2.12131>.
- de Lange, M., von Solms, R., 2012. An e-Safety Educational Framework in South Africa. *Proc. South. Afr. Telecommun. Netw. Appl. Conf. SATNAC* 6.
- Donegan, R., 2012. Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis 3, 33–42.
- e-Safe School, 2020. About the eSafe school Programme | eSafe school [WWW document]. URL <https://esafeschool.ae/about/> (accessed 12.31.20).
- Footy, M., Challenor, L., Murphy, H., O'Higgins Norman, J., 2018. The anti-bullying procedures for primary and post-primary schools in Ireland: What has been achieved and what needs to be done? *Bild. Erzieh.* 71, 88–97. <https://doi.org/10.13109/buer.2018.71.1.88>.
- Footy, M., Samara, M., El Asam, A., Morsi, H., & Khatatab, A. (2017a). A review of cyberbullying legislation in Qatar: Considerations for policy makers and educators. *Int. J. Law Psychiatry*, 50, 45–51. <https://doi.org/10.1016/j.ijlp.2016.10.013>.
- Footy, M., Samara, M., & Norman, J. O. (2017b). Bullying and cyberbullying studies in the school-aged population on the island of Ireland: A meta-analysis. *The British Journal of Educational Psychology*, 87, 535–557. <https://doi.org/10.1111/bjep.12163>.
- Gretter, S., & Yadav, A. (2016). Computational thinking and Media & Information Literacy: An integrated approach to teaching twenty-first century skills. *TechTrends*, 60, 510–516. <https://doi.org/10.1007/s11528-016-0098-4>.
- Gupta, S., & Jawanda, M. K. (2020). The impacts of COVID-19 on children. *Acta Paediatrica*, 109, 2181–2183. <https://doi.org/10.1111/apa.15484>.
- Hatzenbuehler, M. L., Schwab-Reese, L., Ranapurwala, S. I., Hertz, M. F., & Ramirez, M. R. (2015). Associations between Antibullying policies and bullying in 25 states. *JAMA Pediatrics*, 169, e152411. <https://doi.org/10.1001/jamapediatrics.2015.2411>.
- Hosani, H.A., Yousef, M., Shouq, S.A., Iqbal, F., Mouheb, D., 2019. A comparative analysis of Cyberbullying and Cyberstalking Laws in the UAE, US, UK and Canada, in: 2019 IEEE/ACS 16th international conference on computer systems and applications (AICCSA). Presented at the 2019 IEEE/ACS 16th international conference on computer systems and applications (AICCSA), pp. 1–7. <https://doi.org/10.1109/AICCSA47632.2019.9035368>.
- Independent Education Union, 2011. CYBER SAFETY – POLICY FRAMEWORK FOR SCHOOLS AND SYSTEMS [WWW Document]. URL http://www.ieuvictas.org.au/files/5213/3163/9445/policy1101_cybersafety.pdf (accessed 7.8.20).
- Jain, O., Gupta, M., Satam, S., & Panda, S. (2020). Has the COVID-19 pandemic affected the susceptibility to cyberbullying in India? *Comput. Hum. Behav. Rep.*, 2, 100029. <https://doi.org/10.1016/j.chbr.2020.100029>.
- Knowledge and Human Development Authority, 2020a. KHDA: About us [WWW document]. URL <https://www.khda.gov.ae/en/about-us> (accessed 12.28.20).
- Knowledge and Human Development Authority, 2020b. Schools [WWW document]. KHDA. URL <https://www.khda.gov.ae/en/schoolsen> (accessed 8.10.20).
- Knowledge and Human Development Authority, 2015. UAE school inspection framework 2015–16 [WWW document]. KHDA. URL <https://www.khda.gov.ae/en/publications/article?id=10204> (accessed 7.8.20).
- Kozma, R.B., Isaacs, S., 2011. Transforming education: The power of ICT policies. UNESCO.
- Kraft, E.M., Wang, J., 2009. Effectiveness of Cyber bullying Prevention Strategies: A Study on Students' Perspectives 3, 23.
- Kritzinger, E., 2016. Short-term initiatives for enhancing cyber-safety within south African schools. *South Afr. Comput. J.* 28. <https://doi.org/10.18489/sacj.v28i1.369>.
- Kusserow, R.P., 2008. The healthcare compliance professional's guide to policies and procedures. HCPPro, Maarblehead, MA.
- Marczak, M., & Coyne, I. (2010). Cyberbullying at school: Good practice and legal aspects in the United Kingdom. *Australian Journal of Guidance and Counselling*, 20, 182.
- McNeal, R.S., Kunkle, S.M., Bryan, L.D., 2016. State-level Cyberbullying policy: Variations in containing a digital problem [WWW document]. *Crit. Exam. Sch. Violence disturb.* K-12 Educ. <https://doi.org/10.4018/978-1-4666-9935-9.ch005>.
- Medina, L. C., Manzuoli, C. H., Duque, L. A., & Malfasi, S. (2020). Cyberbullying: Tackling the silent enemy. *International Journal of Inclusive Education*, 24, 936–947. <https://doi.org/10.1080/13603116.2018.1500648>.
- Olweus, D., 2000. Bullying. *Encycl. Psychol.* Vol 1 487–489. <https://doi.org/10.1037/10516-191>.
- Readiness and Emergency Management for Schools, (2017). Cybersecurity Considerations for K-12 Schools and School Districts 8.
- Redmond, P., Lock, J. V., & Smart, V. (2020). Developing a cyberbullying conceptual framework for educators. *Technology in Society*, 60, 101223. <https://doi.org/10.1016/j.techsoc.2019.101223>.
- Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for cyber security in schools: The human factor. *Educ. Plan.*, 27, 23–39.
- Ryan, S.M., 2017. The internet playground : One school's experience of cyberbullying (Edd). University of Tasmania.
- Shamsi, A.A.A., 2019. Effectiveness of cyber security awareness program for young children: A case study in UAE. *Int. J. Inf. Technol. Lang. Stud.* 3.
- Sharp, S., Smith, P., 2002. School bullying: Insights and perspectives. Routledge.
- Smith, P. K., Kupferberg, A., Mora-Merchan, J. A., Samara, M., Bosley, S., & Osborn, R. (2012). A content analysis of school anti-bullying policies: A follow-up after six years. *Educational Psychology in Practice*, 28, 47–70. <https://doi.org/10.1080/02667363.2011.639344>.
- Smith, P. K., Smith, C., Osborn, R., & Samara, M. (2008). A content analysis of school anti-bullying policies: Progress and limitations. *Educational Psychology in Practice*, 24, 1–12. <https://doi.org/10.1080/02667360701661165>.
- Tabrez, A., 2020. Corona virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and Cybersecurity (SSRN scholarly paper no. Id 3568830). Social Science Research Network, Rochester, NY. <https://doi.org/10.2139/ssrn.3568830>.
- Tas'adi, R., Mudjiran, Gistituati N., Ananda, A., 2020. Cyberbullying in the digital age: A common social phenomenon. Presented at the 2nd international conference innovation in education (ICoIE 2020), Atlantis press, pp. 196–200. <https://doi.org/10.2991/assehr.k.201209.218>.
- Thomas, L. (2010). Cyberbullying: What Counsellors need to know [book review]. *Australian Journal of Guidance and Counselling*, 20, 238.
- UAE Government, 2020. Cyber laws - the official portal of the UAE government [WWW document]. URL <https://u.ae/en/resources/laws> (accessed 1.3.21).

- UAE Ministry of Cabinet Affairs, U., 2019. National Programme for happiness concludes interactive camps for promoting children's digital wellbeing [WWW document]. URL <https://www.mocaf.gov.ae/en/media/news/national-programme-for-happiness-concludes-interactive-camps-for-promoting-children's-digital-wellbeing> (accessed 7.8.20).
- UAE Ministry of Education, U., 2020. Student behaviour management distance learning 2020 [WWW document]. URL https://www.moe.gov.ae/Ar/Legislation/Documents/Student%20Behaviour%20Management_Distance%20Learning%202020_English.pdf (accessed 7.8.20).
- Välimäki, M., Almeida, A., Cross, D., O'Moore, M., Berne, S., Deboutte, G., Sygkollitou, E., 2012. Guidelines for preventing cyber-bullying in the school environment: A review and recommendations. [WWW document]. URL <https://docs.google.com/a/dnschools.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxjb3N0aXMwODAxGd4OjU0MzAwZDdkODI4ZjIwYTE> (accessed 12.29.20).
- Von Solms, R., Von Solms, S., 2015. Cyber safety education in developing countries.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.