

THE ROLE OF CORPORATE SOCIAL RESPONSIBILITY IN PROMOTING CYBERSAFETY AND DIGITAL CITIZENSHIP USING THE CYBERSMART PORTAL IN A SCHOOL SETTING

Dissertation Submitted to



The IIHMR University, Jaipur

for the partial fulfillment for the award of the degree

of Master of Business Administration (MBA)

in

Hospital and Health Management

by

Dr. Sunam Hazarika

Under the Supervision and Guidance of

Ashish Bandhu

(Assistant Professor, IIHMR University, Jaipur)

2023

THE ROLE OF CORPORATE SOCIAL RESPONSIBILITY IN PROMOTING CYBERSAFETY AND DIGITAL CITIZENSHIP USING THE CYBERSMART PORTAL IN A SCHOOL SETTING

Dissertation Submitted to



The IIHMR University, Jaipur

for the partial fulfillment for the award of the degree

of Master of Business Administration (MBA)

in

Hospital and Health Management

by

Dr. Sunam Hazarika

Under the Supervision and Guidance of

Ashish Bandhu

(Assistant Professor, IIHMR University, Jaipur)

2023

DECLARATION BY STUDENT

I hereby declare that this dissertation titled **“The Role Of Corporate Social Responsibility In Promoting Cybersafety And Digital Citizenship using the Cybersmart Portal In A School Setting”** is the bonafide record of my original researchwork. I declare that it has not been submitted to any other university or institution for the award of any degree or diploma. Information derived from the published or unpublished work of others has been duly acknowledged in the text.



Dr. Sunam Hazarika
MBA-Hospital and Health
Roll no.: 1423
Date:



AUSTRALIA
CHINA
COSTA RICA
INDIA
POLAND
ROMANIA
SPAIN
SRI LANKA
SOUTH AFRICA
THE PHILIPPINES
TURKEY
UAE
UK
USA

Date – 18th April, 2023

Certificate of Project Completion

This is to certify that Dr. Sunam Hazarika has completed the CSR Project titled “CyberSmart Awareness” with WNS Cares Foundation, the CSR arm of WNS Global services from the month of 1st February 2023 to 21st February 2023 under the guidance of the WCF team.

The candidate effectively applied Presentation Skills, tutoring skills, Social service, Community outreach and relationship management.

The overall performance of the candidate was excellent during the project execution.

The project is the part of “Ybrant- the WCF Fellowship Program for Leaders of Tomorrow”. The student will be a certified Fellow on completion of the 12-week program.

We wish him/her all the best for the future endeavors.

GOPAL AGRAWAL

Chief Internal Business Officer and Head - CSR

WNS Cares Foundation

Registered Office: PL-10, Gate No. 4,
Godrej & Boyce Complex,
Pirojshanagar, L.B.S. Marg,
Vikhroli (W), Mumbai 400 079
CIN: U93000MH2011NPL212998

Tel: +91 22 6826 2100
wns.com

CERTIFICATE

This is to certify that dissertation titled “**The Role Of Corporate Social Responsibility In Promoting Cybersafety And Digital Citizenship using the Cybersmart Portal In A School Setting**” is a record of the research work undertaken by **Dr. Sunam Hazarika** in partial fulfillment of the requirements for the award of the degree of **MBA (Hospital and Health Management)** from the IIHMR University, Jaipur under my guidance and supervision and her approach to the research study has been sincere, scientific, and analytical.

Mr. Ashish Bandhu
(Professor and Faculty guide)
IIHMR University, Jaipur

Date:

Dr. Mahender Kumar
(Professor and Dean)
IIHMR University, Jaipur

Date:

ABSTRACT

Introduction: The WNS Cares Foundation (WCF), understands the significance of fostering cybersecurity and digital citizenship. With the aim of educating, empowering, and enriching people, WCF has created several programmes to have a long-lasting effect on the lives of young people from disadvantaged backgrounds. This study is primarily focused on the implementation of the CyberSmart programme in a school setting for analyzing the role of corporate social responsibility (CSR) on student advocacy for cybersecurity and digital citizenship. Cyberbullying, identity theft, and other online threats have increased for young people because of technology's rapid advancement and absorption into daily life. By offering a gamified cybersafety portal with quizzes and content catered to kids, instructors, volunteers, and parents, the CyberSmart initiative, created by the WCF, seeks to solve these issues.

Objectives: The objectives of this study were to understand the role of CSR in promoting cybersecurity and digital citizenship and to highlight the key factors that contributed to the success of the Cybersmart project in promoting cybersecurity and digital citizenship.

Methodology: The study used a cross sectional design to provide an understanding of the role of CSR in promoting Cybersecurity and Digital Citizenship awareness through the implementation of Cybersmart project in St. Xavier's Higher Secondary School, Duliajan, Assam. The study population included the students of that school also the students below Grade 3 were excluded and the sample size was 620 participants in total. Data collection utilized the WCF's CyberSmart portal's age-specific quiz certifications. The study was conducted from February to May 2023, and a convenience sampling technique was used to select participants.

Results: The results of the study showed that 620 students succeeded in completing the Cybersmart certification, displaying their dedication in enhancing their cybersafety and online responsibility abilities. It also encourages appropriate online behavior. The study places a major focus on the value of CSR in reducing cyberstalking, raising public awareness of cybersecurity dangers, and considering teachers' psychological and historical backgrounds.

Conclusion: The study's conclusion highlights the importance of CSR in promoting cybersafety and digital citizenship. The achievements of the CyberSmart project and the information learned from the literature review helped to make clear the role of CSR in reducing online risks. By putting the recommendations, such as the requirement for online citizenship and cybersafety education in school curricula, understanding the function of CSR in preventing digital hazards, and periodic evaluation and improvement of educational initiatives, into practice, educational institutions and stakeholders may help students become responsible and safe digital users, creating a more secure online environment for everyone.

Keywords: Corporate social responsibility, cybersecurity, digital citizenship, online safety, online behavior.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Mr. Ashish Bandhu, Assistant Professor at IIHMR University, Jaipur, for his advice, mentoring, and assistance during the entire writing of my dissertation. His expertise, insightful critique, and support were essential in deciding the scope and quality of this study.

I also want to express my sincere gratitude to the entire WNS Cares Foundation staff for their constant assistance and support. Their advice and help have been crucial throughout the dissertation process. They have inspired and motivated me with their dedication to advancing cybersafety and digital citizenship through the CyberSmart project.

I want to sincerely thank each participant and volunteer in this study. The depth and richness of the findings have been greatly enhanced by their willingness to share their experiences and insights.

I am grateful to my family and friends for their patience, inspiration, and support on this journey. Their faith in my abilities has served as a constant source of motivation.

Lastly, I would like to acknowledge the contributions of all the researchers, scholars, and practitioners whose work I have referenced and cited in this dissertation. Their valuable insights and findings have greatly enriched the study and provided a solid foundation for the research.

Dr. Sunam Hazarika

MBA Hospital and Health (2021-23)

TABLE OF CONTENTS

1. Introduction	
1.1 About the organization.....	6
1.2 Background.....	7
1.3 Concept of Cybersecurity and Digital Citizenship.....	7
1.3.1 Global scenario.....	7
1.3.2 Scenario in India.....	8
1.3.3 Need for Cybersecurity and Digital Citizenship.....	9
1.4 Concept of Corporate Social Responsibility (CSR)	9
1.4.1 Relevance of youth in CSR space.....	9
1.4.2 Evolution of CSR.....	10
1.4.3 Importance of CSR in the Digital Age.....	10
1.4.4 Role of CSR in promoting Cybersecurity and Digital Citizenship...	10
1.5 Cybersmart Portal.....	10
2. Literature Review.....	12
3. Research Question.....	23
3.1 Objectives.....	23
3.2 Hypothesis.....	23
3.3 Purpose of the study.....	23
4. Methodology	
4.1 Study Design.....	24
4.2 Study Setting.....	24
4.3 Study Population.....	24
4.4 Study Tools.....	24
4.5 Duration of study.....	24
4.6 Sample size and Sampling technique.....	24
4.7 Data Collection Procedure.....	25
4.8 Operational Definitions.....	27
4.9 Ethical Considerations.....	27
5. Results	
5.1 Cybersmart project.....	28
5.2 Key factors that contribute to the success of Cybersmart project in promoting online safety and digital citizenship.....	29
5.3 Summary of the results.....	30
6. Discussion	
6.1 Comparison with relevant studies.....	31
6.2 Limitations and Strengths of the study.....	31
6.3 Interpretation.....	31
7. Conclusion.....	33
8. References.....	34

LIST OF FIGURES

Fig 1.1- Number of yearly cases of Cybercrime against children and financial losses globally.....	8
Fig 1.2- Cybersmart Portal.....	11
Fig 4.1- Example of entering details in the Cybersmart portal.....	25
Fig 4.2- Cybersmart learning journey.....	25
Fig 4.3- Age-appropriate content for fun and easy understanding.....	26
Fig 4.4- Age-specific quiz.....	26
Fig 4.5- Cybersmart badge and certificate with unique reference ID.....	27
Fig 5.1- Number of certifications in each Grade.....	29
Fig 5.2- Total number of certifications.....	29

LIST OF TABLES

Table 5.1- Total number of Cybersmart certifications.....	28
---	----

ABBREVIATIONS

CSR	Corporate Social Responsibility
WCF	WNS Cares Foundation
MeitY	Ministry of Electronics and Information Technology
NITI Aayog	National Institution for Transforming India Aayog
NASSCOM	The National Association of Software and Service Companies
IAMAI	Internet and Mobile Association of India
SDG	Sustainable Development Goals
NCSA	National Cyber Security Alliance
ISTE	International Society for Technology in Education
NEA	National Education Association
FOSI	Family Online Safety Institute
CERT-In	Cyber Emergency Response Team – India

1. INTRODUCTION

1.1 About the Organization:

WNS (Holdings) Limited (NYSE: WNS) is a leading Business Process Management (BPM) company. They collaborate with clients across 10 industries to build innovative, digitally led transformational solutions utilizing their profound industry knowledge and understanding in technology and analytics. Their reach extends to China, Costa Rica, Sri Lanka, Turkey, the United Kingdom, the United States, India, the Philippines, South Africa, Poland, Romania, and Spain.(1)

WNS Cares Foundation (WCF), the Corporate Social Responsibility (CSR) arm of WNS Global Services, has evolved from a social initiative into a foundation that continues to make a major and long-lasting difference in the lives of underprivileged children and youth via holistic education.(2)

In collaboration with **NASSCOM, Shri Ajay Prakash Sawhney, Secretary of MeitY**, introduced it nationwide in May 2020. To assure a wide audience, WCF has worked with several ecosystem partners since the portal's introduction, including other not-for-profits, state and federal government agencies, educational institutions, and platforms. **Atal Tinkering Labs (NITI Aayog), Tech Mahindra Foundation, Robotex India Foundation, Pratham Infotech Foundation, Hyderabad City Security Council, and Childline India Foundation** are some of WCF's partners for CyberSmart. The CyberSmart programme completed 7000+ certificates in 2 hours, breaking the “**Asia Book of Records.**”(3)

WCF's mission is to Educate, Empower & Enrich. It offers a variety of opportunities, including digital learning through computer literacy programmes, reading skills and vocabulary improvement through static and mobile libraries, academic support through science exhibitions and math Olympiads, and many other programmes, to help have an impact on more than 540,000 kids throughout most locations where WNS is present.

More than 1lakh underprivileged students from 272 schools in 12 countries are impacted annually by the WCF's suite of programmes. Since 2011, the profoundly transforming programmes have made a difference in many aspects of the participants' life. According to Section 125 of the Companies Act of 1956, it is registered as a not-for-profit organization.

1.2 Background:

The rapid growth of technology in the modern world has created many advantages and opportunities, but it has also created new threats and obstacles, particularly for young people navigating the online world. Cybersecurity and good digital citizenship are becoming big challenges for individuals, groups, and the entire society because of the increase in social media and internet use. Children's usage of the internet and digital gadgets has grown exponentially throughout the world and doesn't appear to be slowing down anytime soon. Cybercrime is a huge concern as society continues to shift towards the digital sphere and often loses corporations tens or even hundreds of millions of dollars. In addition to financial costs, critical infrastructure, societal cohesion, and mental health are at stake.

1.3 Concept of Cybersecurity and Digital Citizenship:

“Cybersecurity” is the technique of guarding against unauthorised entry, assaults, and destruction of digital information, computer networks, and systems. Implementing methods and strategies to stop, identify, and react to possible threats like malware, hacking, data breaches, and other cybercrimes entails putting these measures and plans into practise. Cybersecurity seeks to preserve the privacy, availability, and integrity of digital assets, ensuring the safety of people, businesses, and even entire societies in the digital sphere.

Utilising technology and digital resources ethically and responsibly are referred to as **“Digital Citizenship”**. It entails being aware of and abiding by a collection of values, customs, and conduct that encourage constructive participation, safety, and respect online. Digital literacy, online etiquette, privacy protection, critical thinking, ethical social media use, and the capacity to access and assess digital information are just a few of the characteristics that make up digital citizenship. It places a focus on cultivating the knowledge, abilities, and attitudes necessary for people to participate responsibly in the digital society.

Some reputable organizations and resources related to the concepts of cybersecurity and digital citizenship are:

- National Cyber Security Alliance (NCSA)
- Center for Digital Citizenship at Syracuse University
- International Society for Technology in Education (ISTE)
- National Education Association (NEA)
- The Family Online Safety Institute (FOSI)

1.3.1 Global scenario:

Concerns regarding online safety and cybersecurity are growing along with children's internet usage. A survey by the online privacy and security business - Surfshark (4) found that 58% of parents worldwide are concerned about the safety of their children online. Additionally, according to the survey, 68% of parents think their kids are more likely than they were to be exposed to inappropriate online content. A growing concern is cyberbullying, with 34% of parents saying that their child has been the victim of it. In addition, the survey revealed that 30% of parents think their child had interacted with an internet stranger. These figures emphasise the value of educating kids about cybersecurity and online safety to shield them from potential dangers and ensure that they can use the internet safely and responsibly.

Fig 1.1: Number of yearly cases of Cybercrime against children with financial losses globally



1.3.2 Scenario in India:

Even among families that had been the least inclined to utilise digital technology before to the COVID-19 epidemic, there was a discernible increase in use. In India, 15% of those who frequently use the Internet are under the age of 11. According to **IAMAI**, (5) there are 66 million Internet users in India between the ages of 5 and 11. Through the devices of their family members, they access the Internet. As of March 31, 2019, India has 451 million monthly active Internet users, placing it second in terms of population behind China. Nevertheless, given that just 36% of people utilise the Internet, there is a huge potential for development (5) .

Due to the country's fast technological advancement and pervasive internet use, cybersecurity and digital citizenship are becoming more and more significant. The nation must contend with problems like identity theft and cyberbullying. To improve cybersecurity, the government has put into place programmes including the **National Cyber Security Policy, 2013** (6) and the **CERT-In** (7).

There is a growing understanding of responsible online behaviour and privacy protection as part of encouraging digital citizenship. Education institutions and non-profit groups make an active effort to improve digital literacy and equip people, especially students, with the skills they need for a secure online environment. Tools, guidelines, and awareness campaigns are provided by organisations like the **Cyber Swachhta Kendra** (8) and the **Cyber Peace Foundation** (9) to promote cybersecurity awareness.

However, problems persist. There are issues with inadequate infrastructure, a lack of understanding, and low enforcement of cyber laws. Equal access and the development of digital citizenship still place a high focus on bridging the digital gap, particularly in rural regions. To guarantee a safe and responsible digital environment in India, ongoing cooperation, investment, and policy frameworks are required.

1.3.3 Need of Cybersecurity and Digital Citizenship:

There is no doubt about how technology has become an indelible fixture in modern society so much so that even our daily routines are now deeply entwined with computerized devices and digital services. While this shift has yielded many benefits over time there exist certain complications exclusive to younger generations arising from cyberbullying, identity thefts or being exposed unsuitable content; all posing serious threats online for kids' well-being. Therefore, it is essential that parents understand how important it is to educate their children about appropriate conduct on the web - promoting digital citizenship. If we can promote responsible internet conduct within our youth, then we have a higher chance of producing an online community that is safer and more secure. Another crucial part of using technology in today's environment is being a responsible digital citizen. It is crucial to be aware of any potential risks and concerns associated with utilising the internet considering the expanding use of technology. We may develop into responsible digital citizens by being aware of the threats and adopting preventative measures to safeguard our online presence. Beyond online safety, digital citizenship includes knowing and upholding ethical online conduct, respecting intellectual property rights, and being aware of our digital imprint. Exercising personal accountability for our online conduct and ensuring that we use technology in a way that is advantageous to both us and society at large are essential components of being a responsible digital citizen.

1.4 Concept of CSR:

According to the concept of corporate social responsibility, corporations should think about how their decisions will influence the community, the environment, and society. Sustainability and the SDGs are closely related to it.

There is not a single definition of CSR that's accepted by all interest groups, organizations, and academics. The **World Business Council for Sustainable Development(1998)** offers one of the most extensively accepted definitions. This describes commercial social responsibility as “continuing commitment by business to contribute to profitable development while perfecting the quality of life of the workforce and their families as well as of the community and society at large” (10).

In the context of cybersecurity and digital citizenship, CSR plays a crucial role in promoting awareness, education, and protection against the various threats and risks that individuals face online.

According to Section 135, Companies Act 2013 (11), any firm that meets the criteria of *1000 crores or more in revenue, 500 crores or more in net value, or 5 crores or more in net profit* for the immediately preceding fiscal year is eligible for CSR.

The Company can choose the thematic area for CSR activities, from one of the themes mentioned in **Schedule VII (11)**. This broadly covers areas like Education, Health, Environment, Poverty alleviation, Livelihood, Rural Development, Gender inclusion, Protection of Art & Culture, Contributions to PM CARE Fund, Clean Ganga Fund, Swachh Bharat Abhiyan etc. .

1.4.1 Relevance of youth in CSR space:

It is not only the Corporates or Institutions or Organizations but also it is the responsibility of everyone to work towards the betterment of society and the environment. It is not mere charity or sacrifice but is today a dire need for the nation and planet earth. The current generation, which is growing up, is witnessing adverse changes and has an opportunity to understand its causes. Terminologies like pollution, global warming, acid rain, deforestation are commonly heard now.

Like previous generations, the youth of today also aspire to have high incomes with lots of power and independence. CSR gives them a wonderful opportunity to not only aspire for these, but also to give back and be happy and content with their lives.

1.4.2 Evolution of CSR:

The idea of corporate social responsibility has changed throughout time in India. Corporate philanthropy and charity giving have historically been the primary means through which CSR has been implemented, in keeping with the strongly rooted giving and helping culture in Indian society. During the Industrialization era, Mahatma Gandhi's conception of Trusteeship, which held affluent individuals responsible for the benefit of society, further defined this concept.

In 2013, **Section 135 of the Companies Act** was added, creating the legal foundation for CSR in India. The first nation to formally require CSR is India. Since then, the Indian CSR framework has undergone significant modifications to meet governmental requirements. A key piece of law in the country, the CSR Act offered CSR practices structure, effectiveness, and transparency.

CSR has changed for the better since the law's enactment, becoming more strategic and goal focused. It places a strong emphasis on conforming to both **National and SDGs (12)(13)** objectives. The Act has increased the dedication to addressing need-based initiatives and advancing the nation's general development.

Overall, by introducing structure, openness, and accountability, India's CSR Act has changed how CSR is seen and applied. It has opened doors for collaboration and joint ventures, allowing businesses to have a real, palpable impact on society.

1.4.3 Importance of CSR in the Digital Age:

In the age of digitalization, the value of CSR has become even more clear. As technology continues to revolutionize how we live, work, and communicate, businesses are under growing responsibility to ensure people's safety and well-being online. One should not undervalue the contribution of businesses to the promotion of online safety and responsible behavior. Companies may make a substantial contribution to raising awareness, offering educational efforts, and developing tools and platforms that promote online safety and foster responsible digital behavior through their resources, knowledge, and influence.

1.4.4 Role of CSR in Promoting Cybersecurity and Digital Citizenship

There are several projects and programmes devoted exclusively to cybersecurity in the area of CSR. These programmes are intended to address the hazards and challenges related to the digital world. Corporations show their dedication to safeguarding people, especially young people, against cyberbullying, online harassment, identity theft, and other digital hazards by investing in cybersecurity projects. In order to build a safer online ecosystem, these projects frequently entail cooperation with educational institutions, non-profit organisations, and governmental organisations.

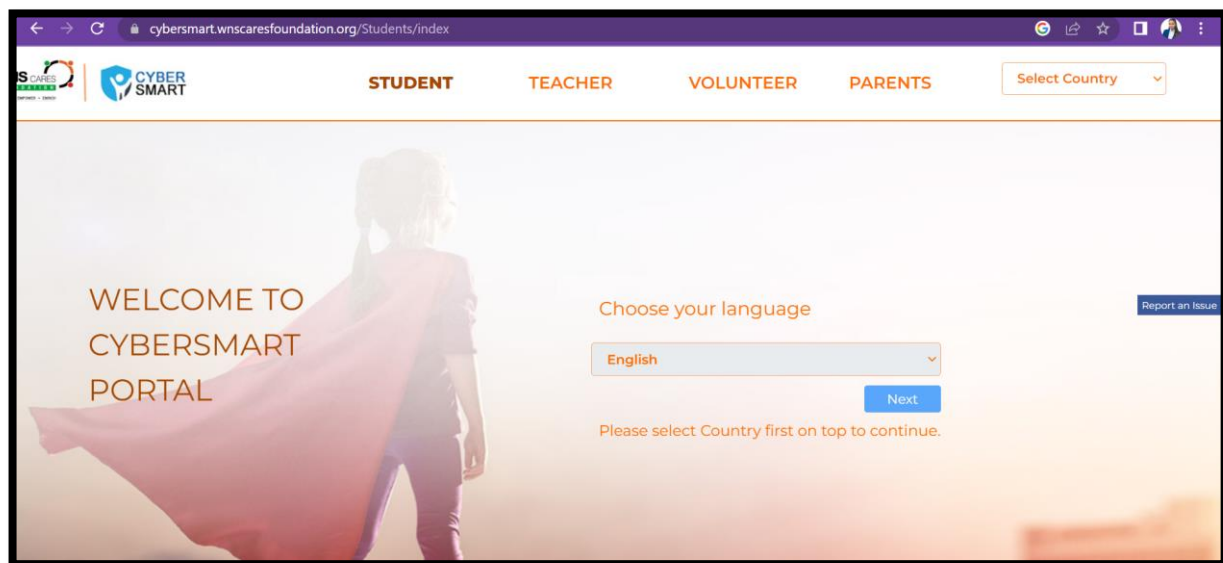
1.5 Cybersmart Portal- Initiative by WNS Cares Foundation:

Cybersmart, a gamified cybersafety portal with age-appropriate content for students as well as customised sections for teachers, volunteers, and parents, is introduced by the WNS Cares Foundation (WCF) to aware people about cyber safety and digital citizenship (14).

Cybersmart is India's first cyber security awareness platform for children. 'Cyber Smart' is a comprehensive cyber safety learning environment developed by WCF for the purpose of educating and empowering kids, instructors, volunteers, and parents. The goal of the Cyber Smart portal is to protect kids online and on digital platforms. The portal is currently available in English & 9 other Indian languages. Importantly, the portal does not collect personal data and can be used by 50,000 individuals at once. It seeks to give kids and teenagers knowledge and skills they need to stay safe online, encourage digital

citizenship, and stop cyberbullying.

Fig 1.2: Cybersmart Portal



2. LITERATURE REVIEW

AUTHOR	NAME OF ARTICLE (YEAR, LOCATION)	METHODOLOGY	FINDINGS
Mahmoud Hawamdeh, Zehra Altınay, Fahriye Altınay, Ahmet Arnavut, Kezban Ozansoy & Idris Adamu	Comparative analysis of students and faculty level of awareness and knowledge of digital citizenship practices in a distance learning environment: case study.(15) (2022, Turkish Republic of Northern Cyprus)	This study used a mixed methods approach, combining qualitative and quantitative methods. Al-Quds Open University in the Palestinian territories and the University of Kyrenia in the Turkish Republic of Northern Cyprus both participated in the research. Faculty members and students from these institutions who met the criteria for the participation requirements made up the study population. Both a survey given to students online and structured interviews with faculty members were used as data gathering strategies. A total of 812 students took the survey, and 16 faculty members were questioned. The Digital Citizenship Scale (DCS) was used in structured online interviews with faculty members to gather quantitative data, which was then manually transcribed and analyzed. For further analysis, the survey information from the students was cleaned, coded, and input into the Statistical Package for Social Sciences (SPSS).	The study's findings showed that both professors and students at Al-Quds Open University (QOU) and the University of Kyrenia (KU) were generally aware of the importance of digital citizenship in distant learning settings. The two colleges' students did exhibit notable differences, with KU students exhibiting a higher degree of awareness and knowledge than QOU students. Despite this, neither student group had a thorough grasp of ideas like digital rights, digital security, or digital ethics. Faculty at QOU demonstrated a greater understanding of digital citizenship, but those at KU emphasized the need to broaden their familiarity with the digital resources and technology accessible. The professors from the two universities did, however, concur that it was critical to include digital citizenship in the curriculum for distance learning.
Farzana Quayyum, Daniela S. Cruzes, Letizia Jaccheri	Cybersecurity awareness for children: A systematic literature review(16)	According to the recommendations made by Kitchenham (2004), a systematic review of the literature on children's cybersecurity awareness	The study discusses findings and knowledge gaps in children's cybersecurity awareness. Privacy, cyberbullying, and exposure to inappropriate information

	(2021, Norway)	research was undertaken in this study. They looked through several electronic databases and manually searched Google Scholar. The study concentrated on qualitative or quantitative works written in English that dealt especially with kids. Studies written in other languages, articles with little empirical support, editorials, article summaries, and other items were excluded using exclusion criteria. In accordance with a predetermined process, the review examined 56 chosen studies out of the 1544 original citations. Finding pertinent research, assessing them, and extracting important data using a template were all steps in the data gathering process.	were the three risks for children that were most commonly highlighted among the 56 publications that were chosen, while other issues received less attention. Although some of the privacy issues were solved, more research is necessary given the understanding of other unique issues. The report emphasizes the necessity for more research into these less well-known risks. It also implies that combining knowledge of cybersecurity with learning and motivational theories might improve efficiency. Numerous strategies, including education, gamification, interventions, and alerts, have helped raise public awareness of cybersecurity, but evaluating their efficacy demands a formal framework, which is still being developed in this area. The study's conclusions can direct further investigation and the creation of focused educational programmes aimed at raising children's cybersecurity awareness.
Haider M. al-Khateeb, Gregory Epiphaniou, Zhraa A. Alhaboby, James Barne s, Emma Short	Cyberstalking: Investigating formal intervention and the role of Corporate Social Responsibility. (17) (2017, Bedfordshire, UK)	This study used both qualitative and quantitative methodologies in a mixed-methods approach. The primary means of gathering data for the study were an online survey and online poll. The study was promoted in several ways, such as awareness events, social media sites, and partnerships with groups like the Network for Surviving Stalking (NSS) in the UK. People who have endured online abuse	According to the survey, a sizable portion of online harassment occurrences take place over private channels like emails and text messages and phone conversations. Many victims were not aware that they may inform their service providers of these instances. While it was widely agreed that the Police should be contacted first, a sizable percentage of individuals chose not to do so for a variety of reasons, including self-blame, guilt, and fear. Those who informed

		made up the research population. With 305 respondents, 274 of whom had experienced online abuse, the online poll gathered both qualitative and quantitative data. Participants responded to survey questions that included both multiple-choice and Likert-type scales for numeric data as well as text/area boxes for qualitative data, as part of the data gathering method.	service providers of occurrences received little to no assistance. Most participants agreed that third parties should step in to handle the threats of cyberstalking; the Police and network providers were the top candidates, but an independent anti-stalking organization was preferred.
Isabel-María García - Sánchez, Alejandra García-Sánchez	Corporate Social Responsibility during COVID-19 Pandemic.(18) (2020, Spain)	The CSR practises of Spanish listed businesses on the Madrid Stock Exchange were examined in this study using a content analysis approach. The study concentrated on 159 businesses that were chosen based on their resources and ability to develop CSR initiatives that benefited Spanish society. As a research tool, content analysis of corporate websites and media sources was employed to compile data especially pertaining to CSR activities during the COVID-19 epidemic. 100 businesses who published information about their CSR initiatives on their websites or in the media made up the final sample, which was chosen using a non-probabilistic selection approach. The process of gathering the data required reviewing the websites of the businesses, paying close attention to the portions that described their strategy, plans of action, and backup plans in the event of the COVID-19 pandemic.	The study found that Spanish companies during the COVID-19 pandemic can be grouped into three clusters based on their corporate responsibility actions. The first emphasizes safeguarding their financial interests, with some individuals also including moral or charitable deeds for public perception. The second consists Leaders in CSR who have made noteworthy contributions to the fields of food, medicine, and research. The third mixes CSR with business ventures, especially in the technology and financial industries. The study shows potential biases in depending on website data and emphasizes the necessity of merging CSR and open innovation projects to combat pandemic threats. To evaluate firm commitment during crises like COVID-19, future study should examine numerical data from non-financial reports.

Moonsun Choi, Dean Cristol, Belinda Gimbert	Teachers as digital citizens: The influence of individual backgrounds, internet use and psychological characteristics on teachers' levels of digital citizenship.(19) (2018, The Ohio State University, USA)	This study was carried out in 14 U.S. states, Washington, D.C., and Puerto Rico using a cross-sectional design. Participants in the Mobilising National Educator Talent (mNET) programme of the U.S. Department of Education, which aims to train 1,500 teachers with alternative credentials, made up the study population. The major data gathering method for the study was an online survey, with a sample size of 348 responses out of 426 survey takers. To choose the participants, convenience sampling was utilised. Giving participants a link to an online survey that asked about their characteristics, teaching experience, and usage of the Internet and social networking sites (SNSs) for teaching purposes served as the data gathering technique.	According to the study's findings, teachers scored better on most of the subscales of the Digital Citizenship Scale (DCS), except for Internet Political Activism (IPA), indicating that they had a moderate level of digital citizenship. Digital citizenship and online self-efficacy (ISE) were positively correlated, however there were weaker negative correlations between some subscales and online anxiety (IA). Except for Technical Skills (TS), factors including personal histories, internet use, and psychological characteristics affected teachers' digital citizenship. Internet-related metrics were used to predict Local/Global Awareness (LGA), Networking Agency (NA), and Internet Political Activism (IPA), whereas backgrounds, internet use, and psychological characteristics were factors in IPA. Overall, there were a variety of ways in which teachers' backgrounds, internet use, and psychological characteristics affected their levels of digital citizenship, with Internet self-efficacy being a key factor.
Sonia Livingstone, Peter K. Smith	Annual Research Review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital	This study employed a systematic review of the literature in the digital environment, concentrating on the online and mobile technologies used by kids. The population of the study includes papers, articles, and pertinent publications that looked at the damages incurred by young users of these technologies. Studies that	According to the study's findings, less than 20% of kids are exposed to dangers including pornography, sexual messaging, cyberbullying, and interaction with strangers. Despite more people having access to internet and mobile technologies, there hasn't been a discernible rise in the prevalence of these dangers, which range in estimates based on definitions and

	age.(20) (2014, London, U.K.)	didn't concentrate on kid users or didn't expressly address sexual and violent hazards in the digital era were excluded. With no set sample size or groups, the study used a systematic search method to find and evaluate pertinent material. Based on predetermined criteria, relevant research papers, reports, and publications were found and chosen for data collection, with an emphasis on the nature, prevalence, and management of these hazards.	evaluations. This may be the result of effective safety education and awareness campaigns or because using mobile and internet technologies does not present higher hazards than using them offline. Even while not all instances of online dangers result in self-reported damage, longitudinal research reveals that they might nonetheless have negative emotional and psychological repercussions. Children are particularly susceptible to these dangers due to a variety of variables, including personality characteristics, psychiatric problems, social factors, and technological concerns.
Oleksandr V. Petryshyn, Oleh S. Hyliaka	Human Rights In The Digital Age: Challenges, Threats And Prospects.(21) (2021, Kharkiv, Ukraine)	The study employed a comprehensive system of scientific cognition methods, including general philosophical and general scientific methods, as well as specific methods from various sciences and legal methods. Analyzing current writings, legal papers, and empirical information about human rights in the digital age was done in an academic setting. As well as basic philosophical techniques like dialectical analysis and synthesis, the study also made use of specialized legal techniques like formal legal and comparative legal analysis. The study used pre-existing literature, court records, and empirical data from several sources, hence the sample size was not defined. To explore the difficulties, dangers, and	Regarding the effect of internet access on human rights, the study emphasizes several important conclusions. It emphasizes how irresponsible behavior and the difficulties of regulating the internet may lead to abuses of human rights. The necessity to identify new rights and reinterpret existing ones to address the changing digital context has increased with the development of digital technology. Digital rights, which include things like freedom of assembly, information access, and digital education, are seen as an extension of fundamental human rights. The issue of whether the right to access the internet constitutes a distinct digital right is up for discussion. The report also focuses on the accountability of online intermediates and the need for precise regulations to control their

		possibilities relating to human rights in the contemporary age, a systematic evaluation and synthesis of research, legal documents, and empirical evidence were used in the data gathering approach.	operations. Digital technology, particularly algorithmic practices, have the potential to both reduce and reinforce prejudice. Due to the widespread use of search engines and information platforms, privacy and data protection have become essential issues, generating worries about user control and privacy. Concerns about individual liberties and the foundations of democracy are further heightened by state control over information that is available to the public and on social media. New technologies have an influence on labor law as well, with arguments on the right to disengage from digital gadgets after hours. Environmental law, administrative law, and government engagement in the digital world are all impacted by digitalization. The report acknowledges Ukraine's active involvement in the digital transformation process, as evidenced by programmes like the Ministry of Digital Transformation and ambitions for the expansion of the digital economy. The report's conclusion states that by balancing the neutrality and accessibility of digital technology with the universality of human rights, it is possible to guarantee people's safety and dignity in the digital era.
Iolie Nicolaidou and Agnes Venizelou	Improving Children's E-Safety Skills through an Interactive Learning Environment: A Quasi-	The study used a pre-test, post-test control group strategy using a quasi-experimental design. Three elementary schools with access to computer labs hosted the experiment. Students in sixth grade	The study found that : The project's goal was to provide instructional materials for teaching young kids e-safety skills. The results of the evaluation of the web-based learning environment "Be Smart when

	Experimental Study.(22) (2020, Cyprus)	(aged 11 to 12) made up the study population. A learning environment with a pre-test, instructional portion, and post-test called "Be Smart When Online!" was one of the study tools. It had multimedia components such movies, photos, presentations, interactive activities, and discussion forums. A written exam with open-ended questions, an online test testing e-safety abilities, a questionnaire measuring student attitudes, and a student interview procedure with open-ended questions were also used. The study time was divided into two 80-minute classes, although the exact dates were not given. The control group, made up of 25 students (14 males, 11 girls), was randomly chosen, whereas the experimental group was made up of 48 students (26 boys, 22 girls). The experimental group was given access to the learning environment, the same online assessments were given to both groups, and four different data sources—including an online test, a paper test, a questionnaire, and student interviews—were used in the data gathering process. Based on the results of the pre- and post-tests, the efficacy of the learning environment was assessed.	Online!" revealed that the experimental group performed much better than the control group in terms of e-safety skills, with a substantial effect size. Interviews with students confirmed the importance of the learning environment in regard to issues such preventing hackers, safeguarding private information, and cyberbullying. The independence of use of the learning environment demonstrated its appropriateness for both formal and casual learning environments. Students indicated positive attitudes regarding the learning environment, even if the positive wording of the questionnaire may have impacted the findings. The study examined the understudied subject of securing computers from viruses and hackers and evaluated learning effects using benchmark tests. The study shows that the "Be Smart when Online!" learning environment is excellent in teaching young children e-safety skills, but additional generalizable research with bigger and more varied samples is required. It was difficult to directly compare pre-test and post-test interviews in order to assess the influence of the learning environment on students' knowledge based on interview data because of the research design.
Leanne Lester, Donna Cross, Debbie	Encouraging the positive use of technology through	In Joondalup, Australia, the study used a community-based intervention strategy.	The study found that: Cybersecurity and technological proficiency

Terrelinck, Sarah Falconer and Laura Thomas	community engagement.(23) (2016, Australia)	Residents between the ages of 12 and 16 were included in the study population, as were representatives from the local government, educational institutions, youth organisations, and community-based organisations. A literature review, interview schedules, and questionnaires were just a few of the instruments that were employed. Calculations and convenience sampling techniques were used to calculate the sample size for the various research components. Structured interviews, questionnaires, and a literature review were used to gather the data, and qualitative and quantitative methods were used to analyse the data to find themes and trends.	must be prioritized throughout the crucial age of transition to school. In order to effectively tackle cyberbullying, the community as a whole must take a holistic strategy. The initiative, which included young people and stakeholders for broad distribution, was governed by Bronfenbrenner's paradigm. By include young people in the study process, we can improve their wellbeing and give them more power to fight cyberbullying. To spread awareness and fill up knowledge gaps, teaching tools as well as an online parent resource were created. The stakeholder group promoted teamwork, participation from the local community, and resource sharing. The development of accessible resources and successful execution were made possible by enough financing. The project's approach may be used by other local governments with a focus on child and family health. Future studies are required to determine how the initiative has affected knowledge, attitudes, behaviors, and the availability of resources. The "Cybersafety and Transition" programme successfully used a local approach engaging local organizations and government. The initiative was effective in increasing awareness and giving parents, teachers, and the community access to useful information.
Julie	A Case Study of	The teachers of the fifth	The study found that:

Lumpkin Payne	Teaching Digital Citizenship in Fifth Grade. (24) (2016, Tuscaloosa, Alabama)	grade were the main subject of this qualitative case study, which was carried out in the Sunshine School System, a small city in Alabama. Within the educational system, the survey covered eight elementary schools, three middle schools, and one high school. The population of interest was made up of certified fifth-grade instructors who had received the Alabama State Department of Education's "Highly Qualified" rating. The study used semi-structured face-to-face interviews, classroom observations, and lesson plan reviews to gather data. Seven of the sixteen fifth-grade teachers in the Sunshine School System who were volunteers made up the sample size. The participants were chosen via convenience sampling. The interviews were captured on an iPad, then Microsoft Word was used to type the transcription. To evaluate how instructors handled digital citizenship during technology-based sessions, classroom observations and an evaluation of lesson plans for technological objectives connected to digital citizenship were done. To make the collection of study data easier, the researcher kept a notebook in which she recorded her experiences during interviews and classroom observations.	The Sunshine School System's participating fifth-grade teachers did not include any special technology standards into their lesson plans; instead, they mostly used the state standards for the relevant curriculum area. Some set strict constraints on internet use to ensure student safety, while other teachers delegated digital citizenship training to computer teachers. Different teachers were more or less aware of the risks and opportunities associated with the internet; some relied on the school's filters and felt comfortable there. Discussions on cybersafety focused on issues including reliance on computer teachers, teacher supervision of internet use, knowledge of digital traces, and minimal use of social media. In order to reduce possible threats, teachers limited student surfing and held casual conversations on cybersafety as required. The participating teachers mostly concentrated on physical use, making sure documents like iPad agreements and Acceptable Use Policies were completed, rather than actively teaching cybersecurity. Few lecturers emphasised proper citations in cyberethics, which mostly focused on avoiding plagiarism. Because of the limited access to social media sites at school, cyberbullying was not seen as a serious problem at this grade level. In conclusion, teachers of fifth grade in the Sunshine School System used a variety
--------------------------	--	--	--

			of methods to teach digital citizenship. While some relied on computer teachers for more formal teaching, others incorporated casual cybersafety conversations. Cyberethics focused on preventing plagiarism, whereas cybersecurity got little attention. Cyberbullying was not viewed as a serious threat in these classes because of the limited access to social media platforms.
--	--	--	--

To choose the most relevant research articles, a thorough evaluation of the literature was conducted. Starting with a thorough identification of relevant keywords and search terms linked to the study's subject, such as “corporate social responsibility,” “cybersafety,” “cybersecurity,” “youth,” “cybersmart,” and “digital citizenship,” was done. Then, renowned academic databases, such academic journals, books, papers, and online archives, were searched using these terms.

The procedure of the literature review ensured that a broad spectrum of perspectives, ideas, and empirical proof were taken into consideration, allowed for a powerful and detailed qualitative analysis. Our understanding of how CSR promotes cybersafety and cyber citizen has improved as a result of the study's ability to explain and widen its findings using credible research papers.

The study's literature review provided us with new knowledge about several issues, including privacy and security, online citizenship, and CSR. They reveal several important insights. Firstly, students and teachers exhibit a sufficient degree of awareness and knowledge of digital citizenship behaviors in a setting of distance learning. This emphasizes the effectiveness of educational efforts in promoting responsible online behavior.

Additionally, the significance of cybersecurity awareness for children is emphasized with the need to educate them about online threats and equip them with the necessary skills to navigate the digital landscape safely. Corporate Social Responsibility (CSR) initiatives are highlighted as playing a vital role in raising awareness about cyberstalking, promoting responsible online behavior, and providing support to victims. The COVID-19 pandemic has also emphasized the crucial role of businesses in supporting communities, employees, and society as a whole. The study also emphasizes how factors such as personal backgrounds, internet usage, and psychological traits can affect a teacher's level of digital citizenship, highlighting the necessity for professional development programmes to improve teachers' digital citizenship practices. Children who use internet and mobile technologies incur risks, including sexual and violent ones, which emphasize the need for comprehensive measures to safeguard their safety. Protecting human rights in the digital age calls for robust legal frameworks and international cooperation to address challenges and threats related to privacy, freedom of expression, and access to information. It is evident that interactive learning settings help youngsters develop their e-safety skills, highlighting the value of interesting educational resources for promoting cybersafety. Additionally, community engagement is deemed vital in encouraging responsible digital behavior and providing support to individuals navigating the digital landscape safely.

Finally, incorporating digital citizenship education into the curriculum positively impacts students' responsible online behavior and fosters their development as digital citizens. These reviews collectively emphasize the significance of promoting cybersafety, digital citizenship, and corporate social responsibility to address the challenges and risks associated with the digital world.

3. Research Question:

How does corporate social responsibility contribute to promote cybersecurity and digital citizenship, specifically through the implementation of the Cybersmart Project in a school setting?

3.1 Objectives:

- To understand the role of CSR in promoting cybersecurity and digital citizenship in a school setting.
- To highlight the key factors that contribute to the success of the Cybersmart project in promoting cybersecurity and digital citizenship.

3.2 Hypothesis:

The implementation of the Cybersmart project, supported by corporate social responsibility initiatives, has a positive impact on improving online safety practices, promoting digital citizenship, and reducing the prevalence of cyberbullying and other threats among young people.

3.3 Purpose of this study:

The purpose of this research was to examine the ways in which CSR advances cybersecurity and digital citizenship. It specifically concentrated on examining the effects of corporate actions in this area, with a concentration on the Cybersmart Project. It aimed to shed light on the value and efficacy of corporate cybersecurity programmes by analyzing the experiences and outcomes of the Cybersmart Project. The outcomes of this study will help us understand how businesses may actively promote cybersecurity and encourage responsible digital citizenship, resulting in a safer and more welcoming online environment for everyone.

4. METHODOLOGY

4.1 STUDY DESIGN:

The study used a cross sectional design to provide an understanding of the role of CSR in promoting Cybersecurity and Digital Citizenship awareness through the implementation of the CyberSmart Project in St. Xavier's Higher Secondary School, Duliajan, Assam, India.

4.2 STUDY SETTING:

In Duliajan, Assam, a renowned institution called St. Xavier's Higher Secondary School, the study was carried out. Based on its willingness to take part and its execution of the CyberSmart project with the support of CSR initiative by WNS Cares Foundation (WCF), the school was chosen for the field of study. The varied student body of St. Xavier's Higher Secondary School, which has students from a range of socio-economic situations, makes it an ideal setting in which to examine how well the CyberSmart project promotes cybersecurity and digital citizenship. The school offers education from Grades 1 to 12, providing an opportunity to engage with students, teachers, volunteers, and parents who have access to the CyberSmart portal. The study environment at the school enables a thorough analysis of the CyberSmart project's implementation in a real-world educational context, advancing knowledge of the function of CSR efforts in promoting cybersecurity and digital citizenship.

4.3 STUDY POPULATION:

The study population were the students of St. Xavier's Higher Secondary School, Duliajan, Assam.

- **Inclusion criteria:** Students from Grade 3 were included in the study who had computer practical classes.
- **Exclusion criteria:** Students below Grade 3 were not included in the study as they did not have computer practical classes.

4.4 STUDY TOOLS:

WCF's CyberSmart portal's age-specific quiz certifications were used for gathering information about respondents' online awareness and behavior.

4.5 DURATION OF STUDY:

The study was carried out from February to May 2023. The three-month period gave a chance to evaluate the CyberSmart project's execution and collect information on participants' knowledge, comprehension, and behavior related to cybersafety and digital citizenship.

4.6 SAMPLE SIZE AND SAMPLING TECHNIQUE :

The study involved students from Grade 3 and above, out of which 620 participation certifications were achieved. The sample size has been determined to ensure an adequate representation of the target population associated with St. Xavier's Higher Secondary School.

Convenience sampling was employed as the sampling technique to select the school for the study. This method allowed for the selection of participants who were readily available and willing to participate in the research.

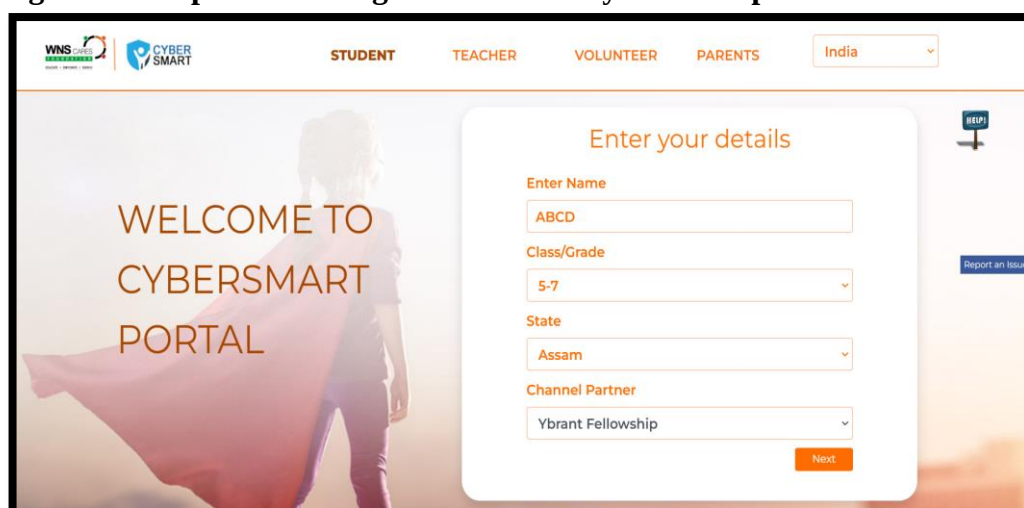
St. Xavier's Higher Secondary School was chosen as the primary study site due to the willingness of the school administration to participate in the study. The convenience sampling technique facilitated efficient data collection within the given time constraints while still providing valuable insights into the effectiveness of the CyberSmart project in

promoting cybersafety and digital citizenship.

4.7 DATA COLLECTION PROCEDURE:

A unique reference ID was created for each participant after they successfully finished and confirmed their success on the Cybersmart site. The class representatives compiled these reference IDs on paper after the researcher gave a list of names organised by roll numbers. To ensure reliable record-keeping, the student lists were taken from the administrative office of the school. The class reps were in charge of obtaining reference IDs from each of their classmates and seeing to it that they were properly documented. These reference IDs were compiled and arranged class and roll number wise in an Excel file. This procedure made it possible to compile an extensive list of the number of students who had earned the Cybersmart certification. The investigator ensured the quality and security of the data gathered from the student representatives by recording the unique IDs in Excel.

Fig 4.1: Example of entering details in the Cybersmart portal.



The screenshot shows the Cybersmart portal registration page. The header includes the WNS CyberSmart logo and navigation tabs for STUDENT, TEACHER, VOLUNTEER, and PARENTS. A dropdown menu shows 'India'. The main content area features a large image of a child in a superhero cape with the text 'WELCOME TO CYBERSMART PORTAL'. To the right, a form titled 'Enter your details' contains the following fields: 'Enter Name' (text input with 'ABCD'), 'Class/Grade' (dropdown menu with '5-7'), 'State' (dropdown menu with 'Assam'), and 'Channel Partner' (dropdown menu with 'Ybrant Fellowship'). A 'Next' button is at the bottom right of the form. On the far right, there are links for 'HELP' and 'Report an Issue'.

Fig 4.2: Cybersmart learning journey.

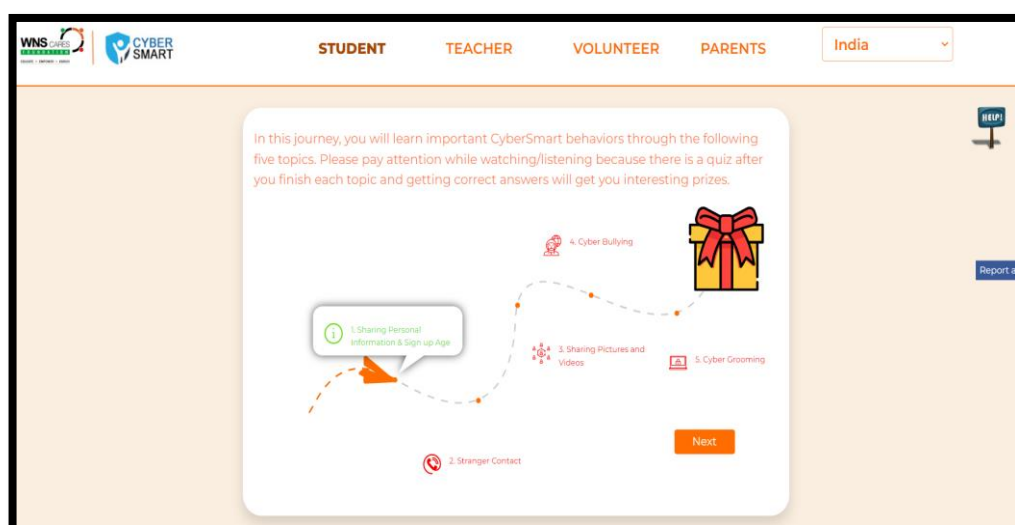


Fig 4.3: Age-appropriate content for fun and easy understanding.

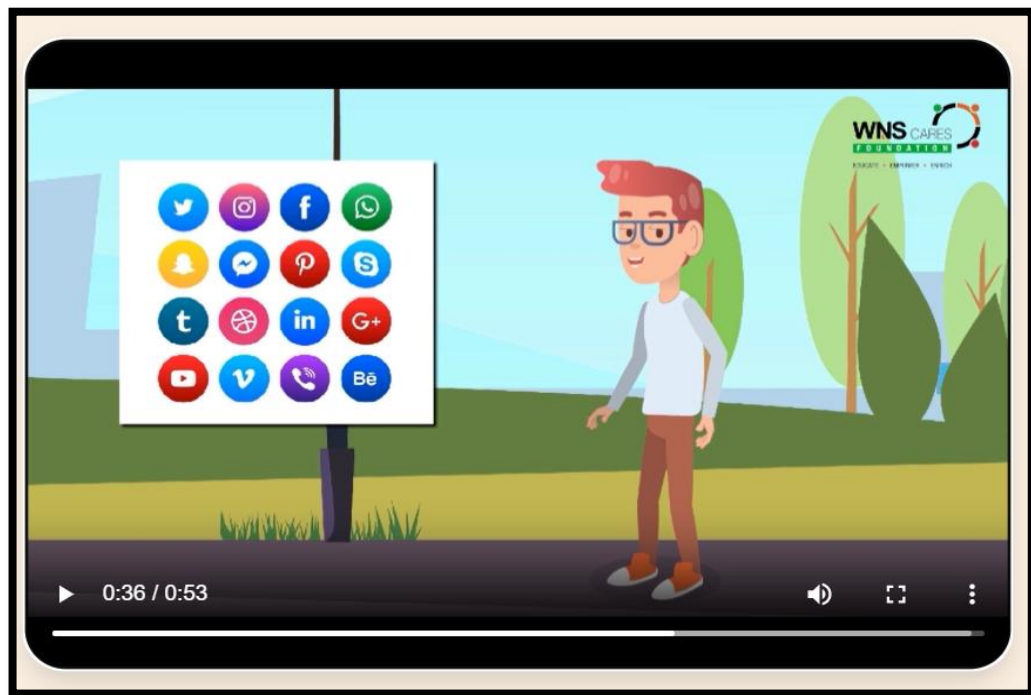


Fig 4.4: Age specific quiz.

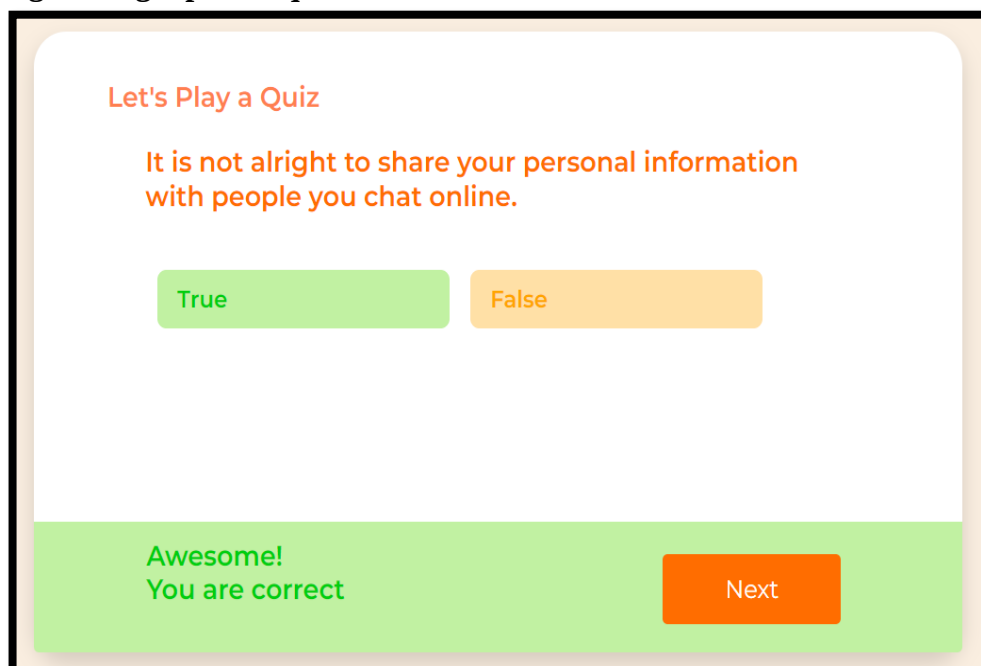
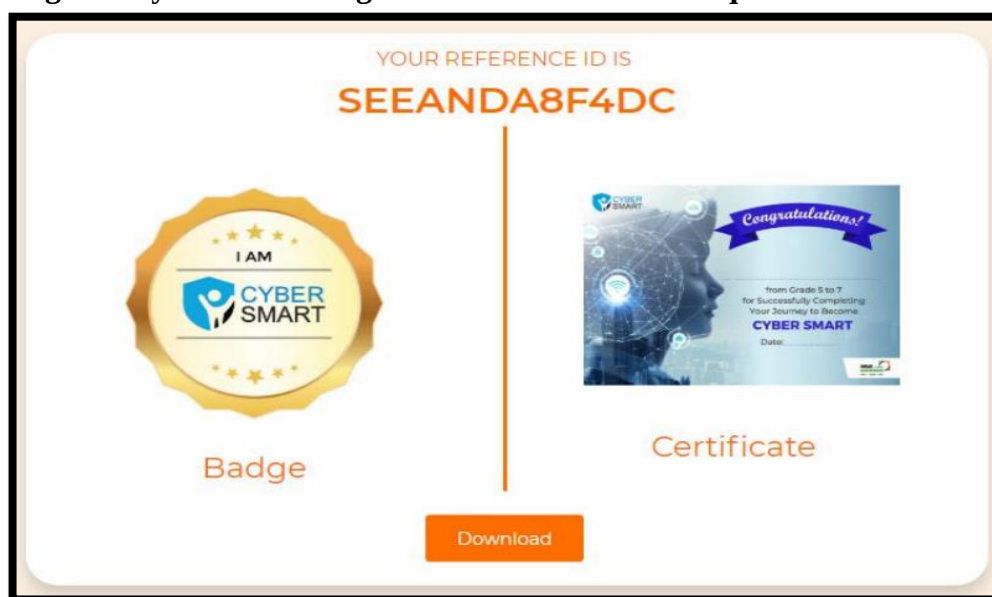


Fig 4.5: Cybersmart Badge and Certificate with unique Reference ID.



4.8 OPERATIONAL DEFINITIONS:

1. Corporate Social Responsibility (CSR): The term "CSR" in the context of this research refers to the voluntarily selected actions and initiatives taken by enterprises to address social and ethical problems, particularly in relation to promoting cybersafety and digital citizenship. It includes efforts made by organizations to ensure the well-being, safety, and responsible behaviour of individuals in the digital realm.
2. Cybersecurity/ Cybersafety: For the purposes of this research, cybersecurity or cybersafety means the skills, knowledge, and procedures that are needed to operate safely in the digital world. It includes having a thorough grasp of the risks and threats that might be present when engaging in online activities, taking precautions to safeguard one's privacy and personal information, and acting responsibly online.
3. Digital Citizenship: In the broader context of the current research, "digital citizenship" refers to the ethical and responsible use of internet resources. It comprises being aware of one's rights and responsibilities in the digital sphere, participating in inclusive and civil online conversation, and exhibiting knowledge of the ethical, social, and legal ramifications of one's online behaviour.
4. Online/Digital/Internet Behaviour: It refers to the choices and actions individuals make when using online platforms, such their observance of moral standards, responsible information sharing, and polite interpersonal contact.

4.9 ETHICAL CONSIDERATIONS:

Informed consent from the Principal of St. Xavier's Higher Secondary School, Duliajan was sought, and they were assured that their information would only be used for the study purpose. No data was shared, and extreme privacy measures were put in place to safeguard personal information.

5. RESULTS

5.1 Cybersmart Certifications: The results demonstrated successful outcomes relating the objectives of the study. More than 600 children received instruction on using the CyberSmart portal, exceeding the intended population sample of 600 participants. About 620 of these students succeeded in completing the certification, displaying their dedication to enhancing their cybersafety and online responsibility abilities.

The respondent's knowledge and comprehension of cybersafety and online responsibility also showed a significant improvement. Students showed improved knowledge and abilities linked to internet safety practices through their use of the CyberSmart website and its age-related assessments. This shows that the CyberSmart project's gamified learning platform was successful in encouraging cybersafety and online citizenship amongst the intended population.

Furthermore, the documentation of reference IDs generated after each child's certification provided a systematic approach to record the progress and participation of the students. This data collection process ensured the accuracy and reliability of the information gathered for analysis and further research.

Table 4.1: Total number of Cybersmart certifications.

Grade	Total number of students in each Grade	Number Of certifications
III	150	66
IV	172	124
VI	135	122
VII	156	116
VIII	150	79
IX	149	45
X	141	68
TOTAL	1053	620

Fig. 5.1: Number of certifications in each Grade

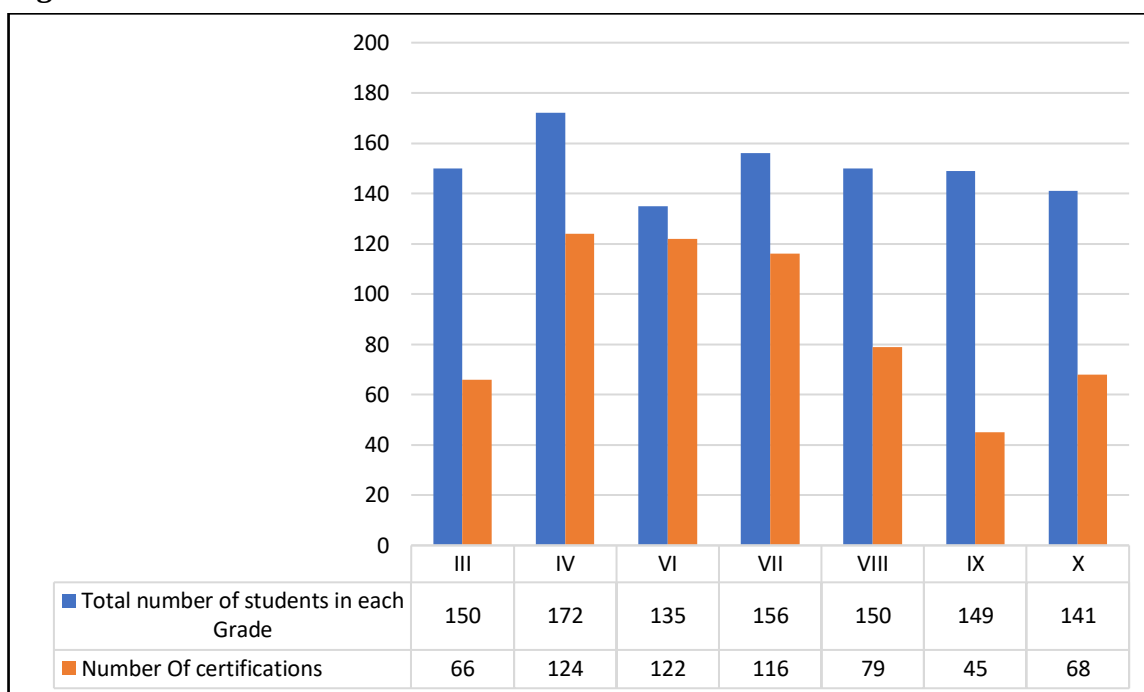
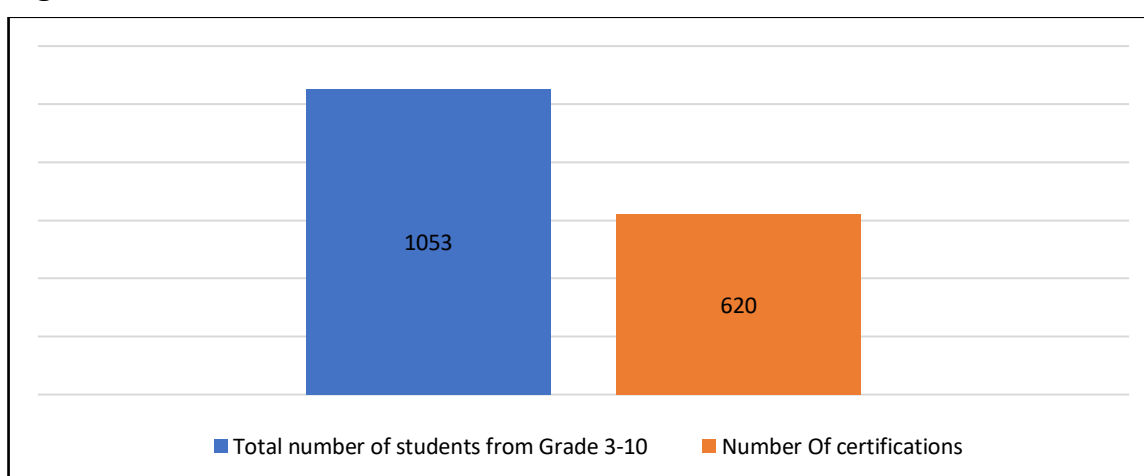


Fig. 5.2: Total number of certifications



5.2 Key factors that contribute to the success of the Cybersmart project in promoting online safety and digital citizenship:

Through the study's objective of identifying the key factors that support the Cybersmart project's success in promoting online safety and digital citizenship was accomplished. The findings identified several important factors that are necessary for the project to succeed. First off, it was observed that the age-appropriate tests and educational materials offered by the Cybersmart portal were successful in raising pupils' knowledge and comprehension of online safety and digital citizenship. The portal's interactive features kept students interested and aided in their learning. Second, it was observed that a key element in promoting and reinforcing the ideas of cybersecurity and digital citizenship was the active participation of teachers and parents. They offered a comprehensive

approach to education in this field through their support and direction.

It was found that implementing the Cybersmart initiative within the school's educational programme was essential for motivating students to develop and uphold responsible digital citizenship and safety practices. These observations provide direction to educational institutions and policymakers in creating a secure and responsible digital environment for kids and indicate the essential success factors for the execution of initiatives of a similar kind.

5.3 Summary of the results:

In general, important new perspectives on how to promote cybersafety, digital citizenship, and corporate social responsibility were identified. The results highlight the significance of these elements in addressing the risks and problems related to the digital environment. The study specifically highlighted the CyberSmart project's success in encouraging students to practice cybersafety and digital citizenship. The encouraging results add to what is already known about the importance of CSR in addressing digital dangers and promoting responsible online behavior. These results offer a direction for the implementation of efforts of a similar nature to build a more secure and safe digital environment for children. The study highlights the significance of ongoing initiatives to promote cybersafety and digital citizenship because of the constantly changing digital world and the rising dependence on technology in many areas of life.

6. DISCUSSION

6.1 Comparison with Relevant Studies:

The research findings of this study shed light on the effectiveness of the CyberSmart project in promoting cybersecurity and digital citizenship among students. To provide a comprehensive analysis, these findings are compared with the results of other studies in the literature.

When comparing the study results with other relevant studies, several similarities and consistencies emerge. For instance, the study conducted by (15) Hawamdeh et al. (2022) based on the comparison of the level of awareness and understanding of digital citizenship practices among pupils as well as teachers in a distant learning context, also found a satisfactory level of awareness and knowledge among participants. This similarity supports the notion that educational initiatives like CyberSmart can effectively enhance digital citizenship practices among students.

Moreover, the systematic literature review conducted by (16) Quayyum, Cruzes, and Jaccheri (2021) based on cybersecurity awareness for children also emphasizes the importance of educating children about online threats and equipping them with the necessary skills to navigate the digital landscape safely. The results of this study support their findings, emphasising the importance of encouraging cybersafety and helping young people identify and mitigate online hazards.

Furthermore, the research by (17) al-Khateeb et al. (2017) based on cyberstalking and the function of CSR, it was discovered that CSR activities can increase awareness of cyberstalking and encourage safe online conduct. The finding demonstrates the usefulness of CSR in addressing cyberbullying and other risks encountered by students, which is in line with the current study's emphasis on the importance of CSR in the CyberSmart initiative.

6.2 Limitations and Strengths of the Study:

It's vital to recognise the study's limitations even if it offers insightful information on how the CyberSmart project promotes cybersecurity and digital citizenship. The conclusion of the study limits the applicability to other educational environments because it was carried out in a particular school environment. Future research should consider a more diverse range of schools and communities to obtain a broader perspective. Also, all the sections of each grade were not able to be covered due to holidays and clash of class timings.

Despite these limitations, the study has several strengths. Firstly, the secondary research approach allowed for a comprehensive analysis of the research objective, providing valuable insights, and understanding of the topic.

Secondly, the survey effectively attracted more participants than the intended sample size of 600, demonstrating a significant representation of the intended audience. Additionally, the research's conclusions showed promising results, demonstrating how well the CyberSmart project promoted students' digital citizenship and cybersafety.

6.3 Interpretation:

The research results highlight the importance of the CyberSmart concept for advancing cybersafety, internet citizenship, and CSR. This interpretation is supported by the research results. The comparison with related studies highlights the findings' consistency across other research undertakings, demonstrating the value of educational programmes in promoting appropriate online activity.

Despite its limitations, the study emphasises the value of ongoing initiatives to promote cybersafety and online citizenship, acknowledging the changing nature of the digital environment and the need for constant adaptation and improvement. The influence of

CSR initiatives and instruction on fostering a responsible digital environment and the need for ongoing adaptation and improvement should be further explored in future studies. Future studies should look more closely at how CSR programmes and educational programmes affect young people's practises for responsible digital behaviour and online safety.

7. CONCLUSION

The goal of the study was to evaluate how CSR works with the CyberSmart project idea in a school context to promote cybersecurity and digital citizenship. The research results provide light on the project's efficacy in promoting responsible digital behavior, improving online safety practices, and lowering the incidence of cyberbullying and other risks among young people.

Consistent evidence about the value of promoting cybersafety, internet citizenship, and social enterprise was found in the literature review. The research under consideration emphasized the value of educational programmes like the CyberSmart project in increasing people's awareness of online hazards, giving them the skills, they need, and encouraging responsible digital behavior. These findings support the conclusions of the current study, showing that the CyberSmart programme successfully encourages students to practice cybersafety and digital citizenship.

The comparison with other relevant studies also highlighted the consistency of the results across different study projects. The successful outcomes of the CyberSmart study supported the effectiveness of instruction in addressing digital dangers and promoting responsible online behavior. These results were consistent with those of earlier research.

For educational institutions, policymakers, and other stakeholders working to promote cybersafety and digital citizenship, the research's conclusions are significant. The success of the CyberSmart programme shows how important it is to integrate programmes like this into school curricula to give students access to a more secure and safer online environment. The results highlight the necessity of continued initiatives to increase public awareness of online hazards, offer instruction on proper digital behavior, and assist those who have been the victims of cyberbullying along with other types of online abuse.

In tackling digital hazards and encouraging responsible online behavior, policymakers should take corporate social responsibility into account. Businesses and organizations can significantly contribute to the development of a safer online environment by actively participating in programmes that support cybersafety or digital citizenship.

The long-term impacts of educational programmes like the CyberSmart programme should be investigated in further research. Studying the results of students that have taken part in such programmes over a prolonged period can offer information about the long-lasting effects on their online safety and behavior.

The need of ongoing review and development of educational efforts cannot be overstated. Programmes like CyberSmart can benefit from regular evaluations of their efficacy, which can assist pinpoint areas for improvement and guarantee that the information is always current with emerging online dangers and technologies.

Academic institutions as well as stakeholders can collaborate to create a safer online environment for children by incorporating the suggestions and findings from this study. In order to confront the difficulties and dangers of the digital world, it is crucial to maintain the dedication to increasing cybersafety, internet citizenship, or CSR.

To provide people, especially children and teenagers, with the knowledge and skills necessary for using the digital world safely and ethically, it is intended that this research will motivate more research and encourage the use of evidence-based practices.

8. REFERENCES

- (1) About WNS [Internet]. Wns.com. [cited 2023 May 24]. Available from: <https://www.wns.com/about-us>
- (2) WNS cares Foundation [Internet]. Wnscaresfoundation.org. [cited 2023 Jun 4]. Available from: <https://www.wnscaresfoundation.org/>
- (3) WCF, NITI Aayog Partner to provide training to Country's Children and Youth on Cybersafety [Internet]. Affairscloud.com. 2020 [cited 2023 Jun 4]. Available from: <https://affairscloud.com/wcf-niti-aayog-partner-to-provide-training-to-countrys-children-and-youth-on-cybersafety/>
- (4) Kids and cybersecurity statistics [Internet]. Surfshark. 2020 [cited 2023 May 24]. Available from: <https://surfshark.com/research/cybersecurity-for-kids/statistics>
- (5) Our Bureau. 66 mn children aged 5-11 years are active Internet users in India [Internet]. Thehindubusinessline.com. 2019 [cited 2023 May 24]. Available from: <https://www.thehindubusinessline.com/info-tech/66-mn-internet-users-in-india-aged-between-5-and-11-years/article29518418.ece>
- (6) Gov.in. [cited 2023 Jun 4]. Available from: https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf
- (7) Indian - computer emergency response team [Internet]. Org.in. [cited 2023 Jun 4]. Available from: <https://www.cert-in.org.in/>
- (8) Csk C-I. Cyber Swachhta Kendra [Internet]. Gov.in. [cited 2023 Jun 4]. Available from: <https://www.csk.gov.in/>
- (9) Cyberpeace.org. [cited 2023 Jun 4]. Available from: <http://cyberpeace.org>
- (10) Muralikrishna IV, Manickam V. ISO 9000, 14000 Series, and OHSAS 18001. In: Environmental Management. Elsevier; 2017. p. 177–208. Available from: <https://www.sciencedirect.com/topics/earth-and-planetary-sciences/corporate-social-responsibility>
- (11) Gov.in. [cited 2023 Jun 4]. Available from: https://www.mca.gov.in/Ministry/pdf/InvitationOfPublicCommentsHLC_18012019.pdf
- (12) National strategies and SDG integration [Internet]. Sdgs.un.org. [cited 2023 Jun 4]. Available from: <https://sdgs.un.org/topics/national-sustainable-development-strategies>
- (13) The 17 goals [Internet]. Sdgs.un.org. [cited 2023 Jun 4]. Available from: <https://sdgs.un.org/goals>
- (14) Tauheed. No title [Internet]. Wnscaresfoundation.org. [cited 2023 Jun 4]. Available from: <https://cybersmart.wnscaresfoundation.org/Students/index>

- (15) Hawamdeh M, Altınay Z, Altınay F, Arnavut A, Ozansoy K, Adamu I. Comparative analysis of students and faculty level of awareness and knowledge of digital citizenship practices in a distance learning environment: case study. *Educ Inf Technol* [Internet]. 2022;27(5):6037–68. Available from: <http://dx.doi.org/10.1007/s10639-021-10868-7>
- (16) Quayyum F, Cruzes DS, Jaccheri L. Cybersecurity awareness for children: A systematic literature review. *Int J Child Comput Interact* [Internet]. 2021;30(100343):100343. Available from: <https://www.sciencedirect.com/science/article/pii/S2212868921000581>
- (17) al-Khateeb HM, Epiphaniou G, Alhaboby ZA, Barnes J, Short E. Cyberstalking: Investigating formal intervention and the role of Corporate Social Responsibility. *Telemat Inform* [Internet]. 2017;34(4):339–49. Available from: <https://www.sciencedirect.com/science/article/pii/S073658531630140X>
- (18) García-Sánchez I-M, García-Sánchez A. Corporate Social Responsibility during COVID-19 Pandemic. *J Open Innov* [Internet]. 2020;6(4):126. Available from: <https://www.sciencedirect.com/science/article/pii/S2199853122011015>
- (19) Choi M, Cristol D, Gimbert B. Teachers as digital citizens: The influence of individual backgrounds, internet use and psychological characteristics on teachers' levels of digital citizenship. *Comput Educ* [Internet]. 2018;121:143–61. Available from: <https://www.sciencedirect.com/science/article/pii/S0360131518300587>
- (20) Livingstone S, Smith PK. Annual research review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age. *J Child Psychol Psychiatry* [Internet]. 2014;55(6):635–54. Available from: <http://dx.doi.org/10.1111/jcpp.12197>
- (21) Journal of the national academy of legal sciences of Ukraine. Vol. 28. National Academy of Legal Sciences of Ukraine; 2021. Available from: [http://visnyk.kh.ua/web/uploads/journals_pdf/%D0%92%D1%96%D1%81%D0%BD%D0%B8%D0%BA%20%D0%9D%D0%90%D0%9F%D1%80%D0%9D%D0%A3_%D0%A2%D0%BE%D0%BC%2028\(1\)_2021.pdf#page=16](http://visnyk.kh.ua/web/uploads/journals_pdf/%D0%92%D1%96%D1%81%D0%BD%D0%B8%D0%BA%20%D0%9D%D0%90%D0%9F%D1%80%D0%9D%D0%A3_%D0%A2%D0%BE%D0%BC%2028(1)_2021.pdf#page=16)
- (22) Nicolaidou I, Venizelou A. Improving children's E-safety skills through an interactive learning environment: A quasi-experimental study. *Multimodal Technol Interact* [Internet]. 2020 [cited 2023 May 22];4(2):10. Available from: <https://www.mdpi.com/2414-4088/4/2/10>
- (23) Leanne Lester Donna Cross Debbie Terrelinck Sarah Falconer Laura Thomas , (2016)," Encouraging the positive use of technology through community engagement ", *Safer Communities*, Vol. 15 Iss 3 pp. 134 - 141 Permanent link to this document: <http://dx.doi.org/10.1108/SC-11-2015-0035>
- (24) Julie LP: A Case Study Of Teaching Digital Citizenship In Fifth Grade. The University of Alabama ProQuest Dissertations Publishing [Internet], 2016. 10239723. Available from: <https://www.proquest.com/openview/9480af7e9df050cf0be7c3cfb310530c/1?pq-origsite=gscholar&cbl=18750>

- (25) García-Sánchez I-M, García-Sánchez A. Corporate Social Responsibility during COVID-19 Pandemic. *J Open Innov* [Internet]. 2020;6(4):126. Available from: <https://www.sciencedirect.com/science/article/pii/S2199853122011015>
- (26) Edition 17th. The Global Risks Report 2022 [Internet]. Weforum.org. [cited 2023 May 24]. Available from: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf