http://aif-doi.org/lnssh/010111

# **Chapter 11: Needs Assessment Research Paper Digital Citizenship**

#### ABDULMALIK ALLUHAYYAN

**Abstract :The** advances in technology we have seen in the past few decades have brought many advantages and disadvantages to society. Technology has changed nearly every aspect of our life from how we interact with friends to how we work. This widespread prominence has created the need for greater awareness of technology's impact and how to use technology effectively and responsibly. **The** term digital citizenship has been coined in order to address these issues and consists of nine elements. This paper will examine digital citizenship from the perspective of Saudi Arabia's education system.

#### Introduction

Today people have never been more connected. Most kids have access to some sort of technological device before they start walking and talking (Schleicher, 2019). Nowadays, parents and teachers face an evolving challenge which is the Internet world. Below is an abstract of a survey that focused on EU kids online in 25 countries and it pointed out the following statistics: Out of nine different types of factors that worry parents about their children being online; 33% of parents worry that their children will be contacted by strangers and 32% of parents worry that their children could be exposed to inappropriate content. These two factors rank 5th and 6th on the survey. Many children were asked if online risks upset them. Out of all the children questioned: 13% of them said they have used reporting tools but only 2/3 found them helpful. In terms of privacy, 43% of children use the private setting, 28% have their settings on practically private and 26% of them have their settings on public. In addition, many public settings expose children's phone numbers or addresses; therefore, privacy settings need to be promoted. The internet is a part of children's daily lives. Statistics show that 93% of children who use the internet go online at least once a week while 60% of children go online every day.

Also, statistics have shown that 14% of children have seen sexual pictures, 8% saw pictures of people having sexual intercourse and 2% of children saw violent, sexual pictures. Out of those children who encountered those images, 22% tried to fix the issue, 19% deleted any unwanted messages and 15% tried to block the sender. But only 13% reported the problem. Excluding sexual content, 21% of children have encountered harmful user-generated content like hate sites, 12% have encountered pro-anorexia sites and 7% have encountered self-harm sites. Unfortunately, only 33% of parents say that they filter their kid's internet usage, 27% of parents claim to use monitoring software but only 27% of parents feel that these strategies are effective in protecting their children online. Regarding cyberbullying, 6% of children have received rude messages, 3% have sent rude messages, and half of those children who were bullied online felt quite upset (Livingstone, et al., 2012). We have evidence that children in Europe face these problems and these problems are a part of the nine elements that are a part of digital citizenship. To protect our children from facing these problems in the future, they should be aware of this.

These are the nine elements that Ribble believes every student should learn. According to (Ribble, 2015, p. 16), these nine elements intend to assist both educators and learners in

Understanding the sections that make up digital citizenship clearer. It also illustrates the pathway for learners to become complete digital citizens.

### **Digital Access**

According to (Ribble, 2015, p. 24,) digital access is "full electronic participation in society." Nowadays, technology allows people to rapidly communicate and connect with one another. However, not everyone has access to technology (Ribble, 2015). Today, children are quite invested in the digital world. In a nationally representative survey, results showed that teachers noticed that students who had access to the internet struggled with the following challenges: problems when communicating with family, problems participating in their school life, and navigating through online learning. Educators from poorer schools mentioned that their students didn't have access to the internet at home. Digital access enabled students to continue with their education through national crises such as war or pandemics (Stelitano, et al.,2020). digital access also allows students with disabilities to enhance their learning. Lastly, it helps to prepare the youth for a technological future (Ribble, 2015).

# **Digital commerce**

Digital commerce is the purchasing and selling of products online. Nowadays, teachers feel that educating students about digital commerce is either too hard or not their responsibility. However, digital commerce has become a significant factor in many people's lives. Therefore, they should be made aware of all aspects of online shopping. For example, if children do not know where or how to buy products on the internet, they can become exposed to scams and identity theft (Ribble, 2015). Another example of the importance of digital commerce is a study that was taken from January 2019 – June 2020 when lego.com became the most popular e-commerce website for children. During this time, lego.com managed to reach an average of 11.1 million views from the US monthly (www.statista.com).

#### **Digital communication**

Digital communication is a quick way in which people communicate with each other virtually. People often use texting applications, phone calls, social media, and emailing platforms to communicate digitally (Ribble, 2015). Even though digital communication has many advantages, it also comes with many disadvantages. Nowadays parents and teachers have noticed that children battle to communicate in face-to-face situations. This is because children who are growing up in the digital age spend as much time on screens as working adults. Parents also say that they don't know how to teach in-person communication as they themselves grew up without these technological devices (Lynch, 2019). Teachers need to keep their student's generation in mind and incorporate appropriate uses of digital communication in their lessons. An example of the appropriate use of digital communication is using social media to support classroom activities and to communicate with parents. While some examples of inappropriate uses of digital communication are using texting platforms to cheat on formal examinations and using social media platforms to cyber-bully other students (Ribble, 2015). In conclusion, educators should help students in Saudi Arabia to prepare them to be able to communicate easily and formally in both the digital and non-virtual world.

# **Digital literacy**

Digital literacy is the understanding of technology and how it works.

In terms of education, learners often enroll in online courses that they find engaging and motivating (Ribble, 2015). We also noticed that digital literacy is evolving, and we should help our students to understand these advancements such as artificial intelligence (Tinmaz et al. 2022, as cited in Kateryna, 2020). Digital literacy is important as the people who were born after 1980 are known as digital natives and have been exposed to technology their entire life. Because of this, learning about digital literacy and gaining the appropriate skills to use technology has become essential for digital natives' lives (Tinmaz, et al., 2022). Critical thinking is another important skill that teachers should help develop in their students (Tinmaz, et al., 2022, as cited in Bawden, 2008). In conclusion, digital literacy should be the foundation of lifelong learning. (Tinmaz, et al., 2022, as cited in Seckin-Kapucu, 2021).

# **Digital etiquette:**

Digital etiquette is the making of digital social norms that are both legal and appropriate. (Faculty of Education, Chiangmai University, 2021) Generally, learners observe how technology is used by others and they learn what is appropriate or not. The problem with etiquette today is that parents don't know what is appropriate when it comes to digital etiquette so they cannot teach their children this topic before they start school. An example of appropriate digital etiquette would be learners learning what information can be shared on their devices in class with their teachers. Educators should teach digital etiquette in school to ensure that all learners are aware of what is considered appropriate and inappropriate (Ribble, 2015).

# **Digital law**

Digital law is the responsibility for a person's actions and dealings online. Nowadays posting, locating, and downloading different materials has become so easy. Unfortunately, when posting content on the internet many people don't think about what is inappropriate or illegal. This becomes a problem when people start to infringe on intellectual property or copywritten material. For example, downloading and exchanging music files illegally (Ribble, 2015). For this reason, I believe that students in Saudi Arabia should study digital law in school. To further explain the importance of learning about digital law in Saudi Arabia; a 2019 survey on cybercrime in Riyadh showed that there were about 3215 crimes that year. This statistic can also be found in the General Authority for Statistics in Saudi Arabia. For example, Table 1 presents the digital laws in Saudi Arabia.

Table 1 shows the digital laws as stated in the Communication and Information Technology Commission statistics.

Any person	Spying on, or	2. Unauthorized	3. Unauthorized	5. Defamation
who commits	interception, or	access with the	access to a	and infliction of
any of the	reception of data	intention of	website, or	damage upon
following	transmitted	threatening or	hacking a	others through
cybercrimes	through an	blackmailing	website to	the use of
shall be subject	information	any	change its	various
to	network or a	person to	design, destroy	information
imprisonment	computer	compel him to	or modify it, or	technology
for a period not	without	take or refrain	• '	devices
exceeding one	Williout	take of ferfalli	occupy its ORD.	

year and a fine not exceeding 500,000 riyals, or either penalty:	legitimate authorization.	from taking an action, be it lawful or unlawful.		
Article 4 Any person who commits any of the following cybercrimes shall be subject to imprisonment for a period not exceeding three years and a fine not exceeding 2,000,000 riyals, or either penalty	1. Acquisition of movable property or bonds for oneself or others or signing such bonds through fraud or the use of a false name or identity.	2. Illegal access to bank or credit data, or data pertaining to the ownership of securities with the intention of obtaining data, information, funds, or services offered.		
Article 5 Any person who commits any of the following cybercrimes shall be subject to imprisonment for a period not exceeding four years and a fine not exceeding 3,000,000 riyals, or either penalty:	1. Unauthorized access with the intention of canceling, deleting, destroying, leaking, damaging, altering, or redistributing private data.	2. Causing an information network to halt or break down, destroy, delete, leak, damage, or alter existing or used programs or data.	3. Obstructing access to, distorting, or causing the breakdown of services by any means.	
Any person who commits any of the following cybercrimes shall be subject	1. The production, preparation, transmission, or storage of material	2. The construction or publication of a website on an information network or	3. The preparation, publication, or promotion of material for pornographic	4. The construction or publication of a website on an information network or

imprisonment for a period not exceeding five years and a fine not exceeding 3,000,000 riyals, or either penalty:	impinging on public order, religious values, public morals, or privacy, through an information network or computer.	computer to promote or facilitate human trafficking	networks or gambling activities that violate morals.	computer to trade, distribute, demonstrate methods of use, or facilitate dealing in narcotic and psychotropic drugs
Any person who commits any of the following cybercrimes shall be subject to imprisonment for a period not exceeding 10 years and a fine not exceeding 5,000,000 riyals, or either penalty:	1. Establishing or publicizing a website on an information network or computer for terrorist organizations to facilitate communication with the leaders or members of such organizations, finance them, promote their ideologies, publicize methods of making incendiary devices or explosives or any other means used in terrorist activities.	2. Unauthorized access to a website or information system directly, or through an information network or computer to obtain data that threatens the internal or external security of the State or its national economy.		

Digital rights and responsibilities

Digital rights and responsibilities are mandatory requirements that are given to people who are a part of the digital world, as well as online freedoms (Ribble, 2015). Teachers should actively have debates

about digital responsibility. They could ask their learners what a certain word means to them, or teachers could talk about temptations they may encounter while surfing the web or social media. Children need to learn about digital responsibility so that they can learn

to differentiate between right and wrong. They also need to learn how to communicate with others in a respectful manner (Fly five, 2021)

#### digital health and wellness

Digital wellness is the act of actively trying to build a healthy relationship with technology in all aspects of one's life (Wikipedia,2017). Educators can encourage health and wellness regarding technology as well as demonstrate how to be safe online so that students can learn from them. It is important to promote digital health and wellness as people can become addicted to being online, harming them physically (Ribble, 2015). To combat developing an online addiction, users need to learn to establish a screen time balance. They can observe how their child reacts after a certain amount of screen time. They can also set a specific time to be online for their child and then stick to that routine. Parents should limit the amount of time they are online in the hopes that their children will copy them. Lastly, families should try to enjoy their screen time together. And just remember, parents should use parental controls in order to monitor what their child can be exposed to online (PHILIPSEN,2019).

# **Digital security**

Digital security is when an online user protects their technological devices from online intruders (Vigderman, Turner, 2022). There are many tools that are used to digitally protect your electronic data such as virus protection software and firewalls. People should also learn to back up their data regularly and find secure websites. Educators should teach students about digital security as students often give away their cellphone numbers, passwords, and personal information without considering what could go wrong. Parents should warn their children about meeting strangers online as children often consider these strangers as friends. If educators and parents fail to teach children about digital security while they're using email platforms, social media, and text messaging platforms; then they will be subjected to phishing or hacking (Ribble, 2015). Hacking is the action of using your technology-related knowledge to break into someone's device in order to steal their data and exploit their vulnerabilities. Generally, there are three different types of hackers, namely: white hat hackers, black hat hackers and grey hat hackers. White hat hackers hack for ethical purposes; generally, because companies pay them to do so in order to test their digital security. On the other hand, black hat hackers hack illegally and usually for bad intentions. Grey hat hackers also hack illegally but their intentions are either good or for fun. Hacking aside, there are many ways in which you can protect your phone from hackers.

- 1. Don't try to jailbreak your phone.
- 2. Set your lock screen to switch off sooner.
- 3. Install two-factor authentication.
- 4. Make your password long
- 5. Turn on 'Erase Data'

#### 6. Turn off 'Auto-Fill'

And remember, you can also detect whether a website is safe or not by checking the padlock symbol next to the URL or by checking whether the URL says 'HTTPS' instead of 'HTTP' (Vigderman, Turner, 2022)

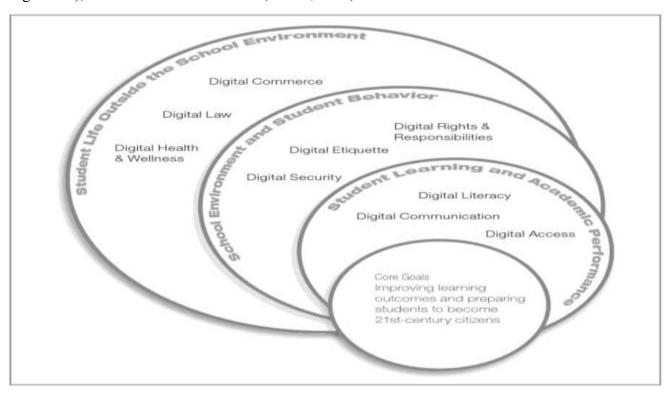
#### **Understanding The Nine Elements**

The nine elements of digital citizenship are not simple, stand-alone issues; they interact in a bewildering array of ways. Based on their stated needs for the normal school environment, these aspects have been

divided into three categories to enable teachers and technology leaders better understand how these various elements interconnect. These groups incorporate the following components:

- "directly affect student learning and academic performance,"
- "affect the overall school environment and student behavior,"
- "affect student life outside the school environment."

Teachers and technology leaders can approach digital citizenship in a way that will directly impact how their school or district uses digital technologies when it is framed in this way (see Figure 2.1), as shown in Ribble's book (Ribble, 2015).



"Fig.2.1 Model of how the elements of digital citizenship relate and connect."

The following passage is from a particular source.

If this were to be taught starting in kindergarten, it would proceed according to the following pattern.

# **Repetition 1 (kindergarten to second grade)**

Respect Yourself/Respect Others

Digital Etiquette

Educate Yourself/Connect with Others

Digital Literacy

Protect Yourself/Protect Others

Digital Rights and Responsibility

# **Repetition 2 (third to fifth grade)**

Respect Yourself/Respect Others

Digital Access Educate Yourself/Connect with Others

**Digital Communication** 

Protect Yourself/Protect Others

Digital Safety (Security)

# **Repetition 3 (sixth to eighth grade)**

Respect Yourself/Respect Others

Digital Law

Educate Yourself/Connect with Others

Digital Commerce Protect Yourself/Protect Others

Digital Health and Welfare (Ribble, 2015).

#### **Conclusion**

In conclusion and to summarize, the study of the above research has shown the importance of digital citizenship and how significant we should be aware to provide a way for our students to be great digital citizens. According to (Ribble 2015, P.66) most public schools in the U.S.A started in the fall of 2014 to teach the nine elements. Therefore, I propose creating a program to teach the nine elements of digital citizenship to Saudi Arabian students, leading them to online life skills

# References

Charin Mangkhang 1 & Nitikorn Kaewpanya 1 2021

The Digital Etiquette Enhancing to Global Citizenship of Social Studies Teachers in a New Normal Society. (n.d.). The Digital Etiquette Enhancing to Global Citizenship of Social Studies Teachers in a New Normal Society. https://files.eric.ed.gov/fulltext/EJ1311721.pdf

Fly Five

DIGITAL RESPONSIBILITY. (n.d.). FLY FIVE. https://www.flyfivesel.org/wp-content/uploads/2021/04/Digital-Responsibility-Article.pdf

Livingstone S,& Haddon L, & Görzig A and Ólafsson K

Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16-year-olds and their parents in 25.

countries. (n.d.). Risks and Safety on the Internet: The Perspective of European Children: Full Findings and Policy Implications from the EU Kids Online Survey of 9-16-Year-Olds and Their Parents in 25 Countries. http://eprints.lse.ac.uk/33731/1/Risks and safety on the internet(lsero).pdf

Stelitano L ,& Doan S, & Woo A,& Diliberti M, & Julia H. Kaufman,& Daniella

The Digital Divide and COVID-19. (n.d.). The Digital Divide and COVID-19.

https://www.rand.org/pubs/research\_reports/RRA134-3.html

Ribble, Mike. (n.d.). Digital Citizenship in Schools: Nine Elements All Students Should Know. Digital Citizenship in Schools: Nine Elements All Students Should Know. https://books.google.com/books?hl=en&lr=&id=z6WpCgAAQBAJ&oi=fnd&pg=PA1&dq=Ribble, +Digital+Citizenship+in+Schools.+&ots=oo\_WVkfmEs&sig=JMHSMsU363RTnZ1Q08Jj-o2yZsA#v=onepage&q&f=false

Livingstone S,& Haddon L, & Görzig A and Ólafsson K

Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16-year-olds and their parents in 25 countries. (n.d.). Risks and Safety on the Internet: The Perspective of European Children: Full Findings and Policy Implications from the EU Kids Online Survey of 9-16-Year-Olds and Their Parents in 25 Countries. http://eprints.lse.ac.uk/33731/1/Risks and safety on the internet(lsero).pdf

Lynch m 2019

How to teach kids to communicate in this digital age. (n.d.). How to teach kids to communicate in this digital age. https://www.thetechedvocate.org/how-to-teach-kids-to-communicate-in-this-digital-age/

Oecd.org

what do we know about children and technology. (n.d.). What Do We Know About Children and Technology. https://www.oecd.org/education/ceri/Booklet-21st-century-children.pdf Philipsen A, 2018

Screen Time Tips For Little Kids. (n.d.). Screen Time Tips for Little Kids. https://puredesire.org/blog/screen-time-tips-for-little-

kids/?gclid=Cj0KCQiA99ybBhD9ARIsALvZavXMVeq\_oj5hcaikHeUsqu-

OVGWMWXg30gliTh\_7RsbVzVhU6M-1OwaApW0EALw\_wcB

Royal Decree "Communication and Information Technology Commission statistics"

file:///Users/malik/Downloads/Anti-Cyber%20Crime%20Law.pdf

 $https://www.statista.com/. \\ (n.d.). \\ Https://Www.Statista.Com/. \\$ 

https://www.statista.com/statistics/1154053/most-popular-children-ecommerce-sites-visits-usa/

Tinmaz H, & Fanea M- & Ivanovici, & Baber H 2022

A snapshot of digital literacy. (n.d.). A Snapshot of Digital Literacy. https://www.emerald.com/insight/content/doi/10.1108/LHTN-12-2021-0095/full/html

Vigderman A, Turner G 2022

A 2022 Guide to Personal Digital Security & Online Safety. (n.d.). A 2022 Guide to Personal Digital Security & Online Safety. https://www.security.org/digital-safety/

Wikipedia. (n.d.). Wikipedia. https://en.wikipedia.org/wiki/Digital health#:~:text=Digital%20health%20is%20a%20discipline,m

edicine%20more%20personalized%20and%20precise.