MASA BRIEF
01
DECEMBER 2022

Policy for Digital Citizenship

Findings from the Family Digital Citizenship in Pandemic Recovery: Prospects, Challenges and Policy Study

NOR DIANA MOHD MAHUDIN
NAZARIAH SHARI'E JANON
MOHD NOOR MUSA

INSTITUT MASA
DEPAN MALAYSIA

THIS PAGE IS INTENTIONALLY LEFT BLANK

NOR DIANA MOHD MAHUDIN

Nor Diana is an Assistant Professor at the Department of Psychology, International Islamic University in Malaysia (IIUM). She is trained in Ergonomics (Human Factors) at Loughborough University and obtained her doctorate in Applied Psychology at the University of Nottingham, United Kingdom. Her research interest include safety interventions, environmental innovations and development, well-being promotion and performance, particularly with regard to digital and online safety, travel behaviour, organisations and workforce, as well as environmental ergonomics.

NAZARIAH SHARI'E JANON

Nazariah is an Assistant Professor at the Department of Psychology, International Islamic University in Malaysia (IIUM). She graduated her doctorate (PhD) program from the School of Psychology, University of Adelaide, South Australia. She has deep interest in psychological development intervention programme particularly are for family, parents, and promote positive social interactions and communications with the adults around them.

MOHD NOOR MUSA

Mohd Noor is a Research Analyst at the Institut Masa Depan Malaysia (MASA). He holds a Master's degree of Science (MSc) in science, technology and sustainability from the Universiti Malaya (UM), Malaysia. Prior joining Institut MASA, he worked at Universiti Malaya and Institut Kefahaman Islam Malaysia (IKIM) on a wide range of research projects and programmes including science and technology (S&T) policy, governance, bioethics, unity and ecotheology in collaboration with various institutions, such as Japan Society for the Promotion of Science, Institute of Future Studies Sweden, Kyoto University, Waseda University and UNESCO Paris.

Executive Summary

The rise of misinformation, online incivilities, hateful speech, and political polarisation during the pandemic has made the acquisition of digital citizenship competence a necessity to create an engaged, informed, and responsible citizenry. However, are families and society prepared to use digital technologies effectively? Furthermore, how can policy be developed to address the rise of ominous trends threatening tolerance, peace, and civility? This study explored these questions in two phases. In Phase 1, 70 documents were reviewed citizenship and analysed, while in Phase 2, 397 parents responded to an online, nationwide survey that gauged the general trends of digital citizenship, self-efficacy, and digital participation and activism. Findings from both phases led to the three policy recommendations as follows:

Key Messages and Recommendations

- Recommendation 1: To legislate digital citizenship
- Recommendation 2 : To make safety by design and responsibility by design as the default
- Recommendation 3: To promote strategies and program that empower rights and responsibilities

Introduction

In the context of online safety, digital technologies, and social media use in children, families have all the responsibility and accountability but no control. On the contrary, service and content providers, telecom operators, media companies, and data brokers have all the control but no responsibility and accountability. What bridges these entities together should be digital citizenship - a concept of how technology impacts people's relationships with others and physical world communities.

At the individual level, digital citizenship refers to the abilities, thinking, and action regarding internet use that allows people to understand, navigate, engage in, and transform self, community, society, and the world (Choi, 2016). At the organisational level, it entails a commitment by the service providers, operators, and companies to take responsibility for the online contents they carry.

A person or organisation that possesses digital citizenship orientation knows about digital rights and responsibilities, is aware of how their online interaction can affect others, has tools to evaluate information obtained from the Internet as truthful or biased, and understands how to communicate in a way that is sensitive to diversity and inclusion.

Negative construction of the impact of social media and digital technologies is so pervasive, and they are talked about as a kind of threat, particularly through the language of risk and crisis. After all, a substantial amount of research has highlighted concerns about screen time and its adverse effects on physical and mental health, education, and overall well-being.

For example, the Microsoft Civility, Safety, and Interaction. Online 2021 report found increased online incivilities during the pandemic, particularly In terms of intolerance in the online community, venting frustrations on networks, and making personal attacks and derogatory comments online.

Other studies also highlighted similar issues wherein social media is misused to spread violent comments, hateful speech, and political polarisation (Castano-Pulgarín et al., 2021; Velásquez et al., 2021). These realities raise two important questions:

(1)
How prepared are families and children to use digital technologies effectively?

(2)
How can policy be developed to address the rise of ominous trends threatening tolerance, peace, and civility?

Several acts, policies, and initiatives have been developed amidst concerns over the adverse impact of digital technologies. Although these resources may provide a good starting place for policy development, they seem to demonstrate a western focus or are confined to educational settings. Also, even when the scope is sufficient, research of similar nature is limited in Malaysia. This poses a problem for understanding the trends in policy goals and implementation strategies for digital citizenship, which is crucial for mitigating online incivilities in children and families.

The Study

This study was conducted in two phases. In Phase 1, acts, policies, and strategies currently available or being developed in Malaysia and other countries are reviewed. Legal documents, policies, guidelines, implementation documents, and scholarly literature published locally and worldwide were gathered with keyword searches such as digital citizenship, digital literacy, online safety, AND family, policy, act, and regulation in publicly accessible databases, legal depositories, and government websites.

70 documents were reviewed and analysed thematically grouping the information within three themes:

- Provisions, features, or elements,
- Strategies, implementations or specifications, and
- Recommendations applicable to digital citizenship policy.

In Phase 2, prevalence data were obtained from a nationwide online survey involving 397 parents (father = 194; mother = 203) to gauge the general trends of digital citizenship, self-efficacy, and digital participation and activism.

Ratings of these variables were obtained using three well-established measures (i.e., Jones & Mitchell, 2016; Ismail et al., 2020; and Choi et al., 2017, respectively).

PHASE 1: WHAT'S MISSING FROM THE CURRENT POLICY OPTIONS?

No Specific Laws on Digital Citizenship

From the documents reviewed, most countries, including Malaysia, have several acts or policies on children, sexual offences, media and broadcasting, transactions, and even some forms of digital literacy. What is lacking, however, is the specific acts or policies that focus on digital citizenship, whether at the organizational, family, or individual levels. In Malaysia, laws are dispersed in various sources, i.e., Communications and Multimedia Act 1998 (CMA 1998), Penal Code, Computer Crimes Act 1997 (CCA 1997), Copyright Act 1997 (CA1997), Personal Data Protection Act 2010 (PDPA 2010), Sexual Offences Against Children Act 2017, and Child Act 2001.

Dispersed law denotes various points of reference, which might dilute the urgency and significance of handling cases. This also means that the dispersed laws that potentially cover digital citizenship can only be applied to the extent of their application; thus, they are inadequate to address high-level risks such as cyberbullying, self-harming, grooming, and pornography.

Consequently, there is a need to address this gap by establishing stand-alone policies and legislations specifically for digital citizenship.

ELEMENTS OF DIGITAL CITIZENSHIP

- Online respect
- Online civic engagement
- Media & information literacy
- Digital access, participation & engagement
- Critical resistance
- Digital commerce
- Digital communications
- Digital literacy
- Digital laws & etiquette
- Digital security
- Digital health & wellness
- Digital rights & responsibilities

Indeterminate Conception and Accountability

In most documents reviewed, there is a tendency to regard digital citizenship as having either;

- Media or information literacy;
- Technical information technology competencies; or
- Digital competencies that focus primarily on using digital services such as banking, e-governance, shopping, and learning in daily life.

These general and indeterminate conceptions of digital citizenship limit the scope of policy development and legislative intervention.

Instead, a more robust definition that focuses on the competencies for being aware of and acting responsibly to maximize goodwill in using digital services, the Internet, technologies, tools, and social media should be adopted.

With the exception of the United Kingdom (UK), another area found lacking in the majority of these documents is the promotion of accountability by service and content providers, social media platforms, telecom operators, media companies, and data brokers in their business practices. These entities profit from content traffic and have massive power in controlling what users are directed to. They have also been made so rich and powerful but with no balancing oversight or societal responsibilities.

As such, there is a strong case to be made, morally, ethically and legally, for these entities to be imposed a duty of care to protect families, especially children, who are using their services from illegal or harmful materials as well as legal but harmful contents. It is also imperative for these entities to carry out substantial and ongoing risk assessments, together with implementing measures to mitigate those risks.

Suppression Rather Than Empowerment

Another prominent theme that arose from these documents revolved around responsibilising people to self-regulate and manage their own digital safety, identity, and reputation. In this context, citizens are directed to a list of qualities defining how to "be a responsible digital citizen". The central message is that in a world where authorities cannot monitor all digital interactions online, citizens must take on some responsibilities to monitor themselves and others to safeguard the community(Johns, 2021). This reliance on people to self-regulate provides an insight into how digital citizenship is conceptualised by policymakers.

This shift in responsibilities has clear implications for the language and tone used to describe digital technology and Internet use. Often, they are discursively positioned as risky, negative, unhealthy, or a problem to be solved. Consequently, intervention programmed and educational curricula are geared towards monitoring and surveillance of digital technology and Internet use as well as obedience to the law.

These practices raise concerns because emphasizing self-regulating, self-policing digital citizens as an outcome of social conditioning and educational interventions can suppress human rights dampen people's willingness to exchange ideas online, close up civic spaces and collective actions, and quell legal dissents.

In fact, digital user rights were largely absent in the discussion of current policies or frameworks. Where rights were mentioned, the focus usually fell on the provisions of digital access, digital inclusion, and privacy rights.

What is needed, therefore, are policies that will drive the development and deployment of intervention programmes and educational curricula that safeguard and empower users, particularly children and families. In this context, it means empowering people to understand their rights and responsibilities as digital citizens.

Detachment from Current and Future Realities

There has been a growing, global trend towards policies and discourses that emphasise the roles and responsibilities of all stakeholders to consider safety by design. United Kingdom, Australia, Singapore, and some states in the United States have started to draft and prioritise an Online Safety Bill for their countries. This Bill is wide-ranging legislation that aims to:

- create safer online spaces for adults and children,
- protect freedom of expression, and
- promote innovation by regulating technology and social media companies a legal duty to prevent and remove harmful contents.

This Bill is also envisaged to address issues arising from provisions scattered across different jurisdictions.

In this review, we found that many countries, including Malaysia are somewhat behind compared to developed countries in drafting the said Bill. This means that our existing policies do not reflect the current and future realities.

Policies are living documents that should evolve with the times and, thus, should be updated or changed to mirror and anticipate these realities.

The Technology is There But The Impacts of the Applications Are yet to be Properly Understood

Although monitoring, self-regulation, and legislation are critical in digital citizenship, it is also the responsibility of the technology companies and social media platforms to safeguard the users', especially children's safety in online spaces.

Since these companies are the ones who created, managed, monitored, and controlled the platforms and contents, they have the ability to intercept real-time audio streams, determine offensive materials, put age verification measures in place, monitor real-time online spaces, establish reporting mechanisms and appropriate actions, and provide human moderation of inappropriate contents.

These technologies are already being used for surveillance, monetisation, and control. By the same token, they can be used to protect users from cyber-criminals, cyber-bullies, stalkers, or predators. The question as to why they are not widely used by these companies and platforms to create safe digital environments is a big concern.

The recommended responsibilities should include conducting risk assessment duties, having independent review processes, providing easy-to-access complaint functions, as well as taking proactive and immediate steps to combat illegal contents, contents that are harmful to children, and contents that are harmful to adults.

WHY THESE FINDINGS MATTER?

1. Show consistencies and diversities in digital citizenship-related policies and strategies regionally and globally.
2. Demonstrate how Malaysia compares in relation to other countries.
3. Identify what is lacking in the existing policies and what is needed for the Malaysian government to foster digital citizenship.

PHASE 2: PREVALENCE OF DIGITAL CITIZENSHIP

(1) High Usage, Big Footprint

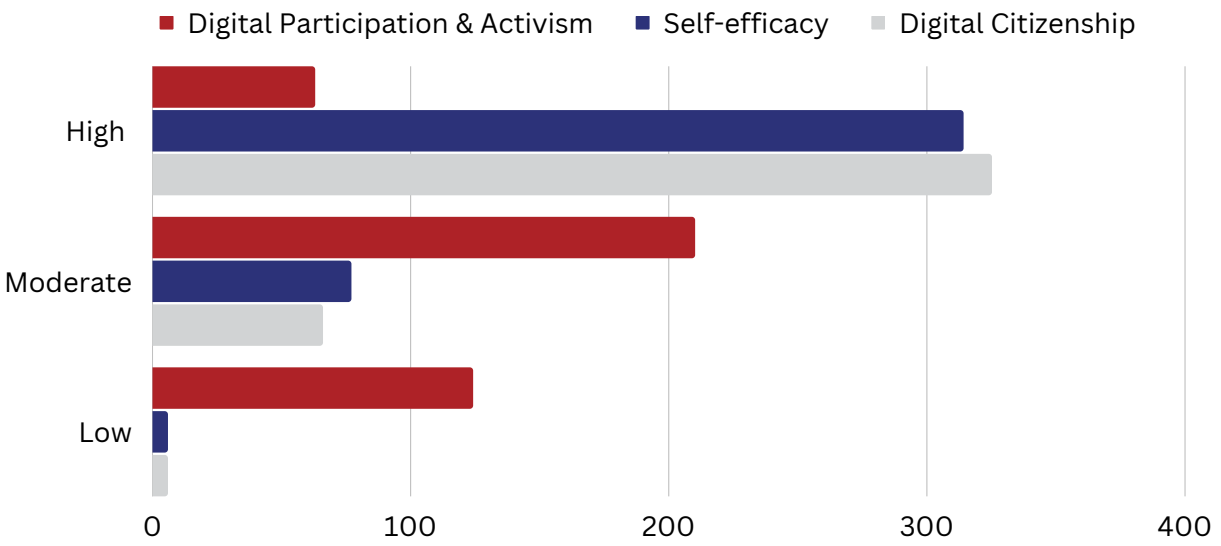
The evidence that young children show high usage patterns indicates that Malaysian children now spend a lot of time using digital devices and the Internet. They do this either via their own online presence or have a digital footprint through their parents.

As such, it becomes vital to include digital citizenship and literacy to assist children and families in developing cyber-resilience - a point that cannot be emphasised enough.

(2) Screen Time, Scream Time

Large proportions of young children in this study have exceeded the recommended screen time. Parents may not be aware of the short and long-term issues linked to excessive screen time, including its effect on children's physical health, eyes, mental health, and overall well-being. Spending more hours on digital devices also means less time outdoors, which is also harmful.

The increased use of technologies and the Internet placed families even more in the spotlight as users. As such, finding ways to foster parents and family knowledge on how best support and protect children online is necessary for current and future family life and relationships.



(3) Parents' Digital Citizenship

The high digital citizenship among parents reflects the growing awareness about their child's digital devices use and suggest that parents may want to find ways to mediate their child's devices and internet usage.

It is likely that this citizenship can be leveraged as a resource that can nudge or motivate the responsible use of technologies in families. Hence, digital citizenship policies and programmes are needed because families, especially children, may risk their personal safety and security, physical and mental health, online reputations, and social relationships because of technology misuse.

(4) Parents' Self-Efficacy

Because digital citizenship depends on parents' responsibility, self-efficacy, policies or programmes for instilling family digital citizenship should specifically focus on parents' self-efficacy to implement the recommended intervention activities.

Parents' self-efficacy here refers to parents' confidence in their general ability and skills to keep their children safe online. Therefore, it is crucial for stakeholders to consider this aspect in any interventions to ensure that they provide effective digital skills to mitigate associated risks arising from the use of digital devices.

POLICY RECOMMENDATIONS

(1) Legislate Digital Citizenship

Since all democratic countries are now working to put in place appropriate, relevant, and effective legislation to ensure respect, tolerance, responsibility, civility, and integrity in online activities, Malaysia should start drafting these legislations accordingly. The government has already shown its willingness to address what happens online with the changes in the Child Act, laws relating to sexual offences, and policies related to computer crimes and cybersecurity.

On this basis, what is needed more is a specific policy that allows quick actions to intervene when changes in digital practices, technologies, or markets create harm or imbalances. This also means making the said policy and legislative processes capable of anticipating the changing contexts of technologies and adapting to them. Because the Internet transcends territorial borders, the laws must also be drafted in tandem with international laws and bilateral or multilateral treaties that uphold the same visions and values to be protected.

(2) Make safety by design and responsibility by design as the default

Online safety is determined by three layers of governance that indicate appropriate technology use:

(i) laws and state regulations;
(ii) platform controls in the form of technical codes and monitoring and flagging tools; and
(iii) application of norms through intervention programmes.
(McCosker, 2015)

As businesses that provide services to children and families, service and content providers, telecom operators, social media platforms, media companies, and data brokers must be responsive to their presence in digital environments. In particular, strategies to reduce the harms that should be adopted need to aim not only at the content level but also at the platforms' infrastructure. They need to develop tools and techniques to support principles such as fairness, explain ability, robustness, accountability and privacy, and build these into their systems and platforms.

The high digital citizenship among parents reflects the growing awareness about their child's digital devices use and suggest that parents may want to find ways to mediate their child's devices and Internet usage. It is likely that this citizenship can be leveraged as a resource that can nudge or motivate the responsible use of technologies in families.

Hence, digital citizenship policies and programmes are needed because families, especially children, may risk their personal safety and security, physical and mental health, online reputations, and social relationships because of technology misuse.

It is also emphasised that these entities must exercise due diligence to detect, identify, prevent, mitigate, and account for how they create, manage, monitor, and distribute the platforms and contents to prevent any harm in digital environments.

This is a part of being responsible by design, i.e., the understanding of the importance of incorporating responsible algorithms and artificial intelligence into the data and strategies across the complete lifecycle of all of their processes and products.

However, disciplining tactics such as giving massive fines for violations or negligence are not recommended because the fines represent a fraction of these companies' annual revenues and are often written off as cost-of-doing-business. Therefore, they fail as a deterrent (Popiel, 2022).

(3) Promote strategies and programmes that empower rights and responsibilities

The focus should also be made to empower and equip families, especially children, with skills to navigate the Internet safely and be responsible users who can distinguish between good and dangerous information in digital environments.

To make this happen, strategies, programmes, and resources supporting digital citizenship must provide all users with the training and skills on how to identify misinformation, manipulation, grooming, and online propaganda. Specifically, users should be:

(i) Informed of the effects of digital technologies on communication and relationships;

(ii) Educated on how to be responsible for their online activities and actions; and

(iii) Provided a clear understanding of responsible use principles and how to translate them into actions.

Conclusion

There is no doubt that we now live in a digital world. Protecting children and families does not mean forbidding them from participating in digital environments.

As a matter of fact, in this century, every child and family should have access to the Internet connection and digital environments and be able to use them “knowledgeably, creatively, and fearlessly” (Kidron, 2018).

Hence, a set of policies and mechanisms needs to be implemented to guarantee a sufficient level of safety and security for every child and protect families from falling into precarious circumstances.

Overall, the findings in this study point to the fact that the internet and digital technologies facilitate daily life activities and enhance everyday communication and maintenance of relationships, especially in extraordinary circumstances, such as the pandemic.

For this reason, the governance architectures for digital environments that allow children and young people would need to consider that through them, families can be trained toward behaving as connected yet ethical and responsible digital citizens.

Key Points

Malaysian children spend much time using digital devices and the Internet, which increasingly have more substantial and longer-lasting impacts on health, well- being, and relationships.

Children are disproportionately at risk due to:

i) the non - existence of policies or legislation on digital citizenship.
ii) strategies that suppress rather than empower.
iii) lack of accountability by service and content providers, operators, social media platforms, and data brokers.

Urgent need to enact stand alone policies and legislations on digital citizenship in Malaysia.

Efforts should focus on legislating digital citizenship, enforcing safety and responsibility by design, and promoting the empowerment of rights and responsibilities.

References

Academy of Child and Adolescent Psychiatry (2020). Screen Time and Children. https://bit.ly/3RR3pjV

Castaño-Pulgarín, S. A., Suárez-Betancur, N., Vega, L. M. T., & López, H. M. H. (2021). Internet, social media and online hate speech. Systematic review. Aggression and Violent Behavior, 58, 101608. https://doi.org/10.1016/j.avb.2021.101608.

Choi, M. (2016). A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age. Theory &Amp; Research in Social Education, 44(4), 565–607. https://doi.org/10.1080/00933104.2016.1210549.

Choi, M., Glassman, M., & Cristol, D. (2017). What it means to be a citizen in the internet age: Development of a reliable and valid digital citizenship scale. Computers &Amp; Education, 107, 100–112. https://doi.org/10.1016/j.compedu.2017.01.002.

Ismail, M. Z. H.,Farid, N. D.N., & Zaki, R. A. (2020). Developing and testing the psychometric properties of the Parental Digital Security (P-Dis) Questionnaire for Malaysian parents. ASM Science Journal, 13(5), APRU 2018, 83-95. https://bit.ly/3aWNWOH.

Johns, A. (2021).“Are we becoming the kind of nation that just blocks out all criticism?”: Negotiating the gap between digital citizenship education and young people’s everyday digital citizenship practices in Malaysia. International Journal of Communication, 15, 4690–4708. http://hdl.handle.net/10453/152615.

Jones, L. M., & Mitchell, K. J. (2016). Defining and measuring youth digital citizenship. New Media &Amp; Society, 18(9), 2063–2079. https://doi.org/10.1177/1461444815577797.

Kidron, B. (2018). Are children more than ‘clickbait’ in the 21st century?. Communications Law, 23(1), 25-30. https://5rightsfoundation.com/uploads/comms-law-23-1-1.pdf.

McCosker, A. (2015). Managing cyberbullying: The three layers of control in digital citizenship. In A. McCosker, S. Vivienne,& A. Johns (Eds.), Negotiating Digital Citizenship: Control, Contest, Culture (pp. 21–40). Rowman & Littlefield.

Popiel, P. (2022). Digital Platforms as Policy Actors. Palgrave Global Media Policy and Business, 131–150. https://doi.org/10.1007/978-3-030-95220-4_7.

Ribble, M., & Bailey, G. (2007). Digital Citizenship in Schools. International Society for Technology in Education.

Savic, M., McCosker, A., & Geldens, P. (2016). Cooperative Mentorship: Negotiating Social Media Use within the Family. M/C Journal, 19(2). https://doi.org/10.5204/mcj.1078.

Velásquez, N., Leahy, R., Restrepo, N. J., Lupu, Y., Sear, R., Gabriel, N., Jha, O. K., Goldberg, B., & Johnson, N. F. (2021). Online hate network spreads malicious COVID-19 content outside the control of individual social media platforms. Scientific Reports, 11(1). https://doi.org/10.1038/s41598-021-89467-y.

Institut Masa Depan Malaysia
192, Jalan Ara, Bukit Bandaraya, 59100 Wilayah
Persekutuan Kuala Lumpur

For more information, visit our website:

www.institutmasa.com

INSTITUT MASA
DEPAN MALAYSIA