

Managing digital citizens: online safety and the rise of private actors in New Zealand schools

Andrew Doyle, Marta Estellés & Dianne Forbes

To cite this article: Andrew Doyle, Marta Estellés & Dianne Forbes (03 Sep 2026): Managing digital citizens: online safety and the rise of private actors in New Zealand schools, Learning, Media and Technology, DOI: [10.1080/17439884.2026.2716045](https://doi.org/10.1080/17439884.2026.2716045)

To link to this article: <https://doi.org/10.1080/17439884.2026.2716045>



© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 03 Sep 2026.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

Managing digital citizens: online safety and the rise of private actors in New Zealand schools

Andrew Doyle , Marta Estellés  and Dianne Forbes 

Te Kura Toi Tangata School of Education, University of Waikato, Hamilton, New Zealand

ABSTRACT

Online safety has increasingly become an issue in schools worldwide. For both teachers and students, online safety problems, from sleep deprivation through to sextortion, present unprecedented challenges beyond the control of school management. The pressing nature of online safety issues combined with other material conditions, such as underfunded public systems and neoliberal administration models, has presented a breeding ground for private organisations to flourish in this field. In this study, we examine how schools enact online safety, the educational approaches underpinning these efforts and the conditions favouring the privatisation of online safety services. The context of the research is New Zealand – a country whose education system has experienced a sharp rise in privatisation over the last few decades. The study draws on ethnographic data with four high schools, involving school leaders, teachers, students and private organisations – for profit and non-profit – providing services to these schools. Our findings point at the unrealistic expectation of demanding schools guarantee young people's safety online and the problems associated with the increasing privatisation of the field, including the lack of critical approaches to digital citizenship education. The article concludes with recommendations for policy makers, including legislative measures to hold online platforms accountable for online harm.

ARTICLE HISTORY

Received 22 September 2025
Accepted 4 August 2026

KEYWORDS

Online safety; schools; New Zealand; privatisation; digital citizenship

Introduction

The safety of young people in the online world has increasingly become a serious day-to-day issue for schools around the world. For both teachers and students, online safety problems, from technological addiction through to cyber bullying, are presenting unprecedented challenges that often escape the control of school management (Dudman 2021; Russell 2021; Tapaleao 2018). While many teachers are aware of the limitations of safeguarding measures and the need to embrace more proactive educational approaches (Webster 2026), schools are under increasing pressure to manage online risks. Particularly since the pandemic, there has been a sharp rise in private actors, including Ed-Tech companies, non-profit organisations and edu-consultants, offering 'solutions' to schools to respond to these complex demands (Williamson and Hogan 2020). These 'solutions' range from the outsourcing of online safety curriculum resources to the use of digital surveillance mechanisms to monitor students, which often have problematic implications for young people's digital citizenship and rights (Estellés and Doyle 2025a; O'Daffer, Liu, and Bloss 2025). This

CONTACT Andrew Doyle  andrew.doyle@waikato.ac.nz Te Kura Toi Tangata School of Education, University of Waikato, 180 Hillcrest Road, Hillcrest, Hamilton 3240, New Zealand

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

privatisation, however, cannot be solely understood as the result of private actors aiming to profit from the public system (Ball 2012; Jobér 2024). They are also facilitated by public policies promoting school autonomy, accountability and competition that are creating quasi-market environments for schools (Ball 2012; Hogan 2025; Verger, Fontdevila, and Zancajo 2016).

There has been, however, little investigation on the specific ways schools respond to online safety, the conditions that are allowing private actors to ‘flourish and expand’ (Ball 2012, 17) and the educational approaches that underpin such online safety efforts. In this study, we explore these issues in the context of New Zealand, where processes of privatisation – both *in* and *of* – the education system (Ball and Youdell 2008) have been quietly intensified and consolidated over the past few decades (Thrupp et al. 2020). As part of this broader trend of privatisation, New Zealand schools are increasingly resorting to external organisations – both for profit and non-profit – to deal with the risks posed by digital technologies.

In this article, we begin our investigation by problematising common educational responses to online safety and outlining our conceptual framework for the analysis of online safety educational responses. Following this, we engage with scholarship on online safety at schools and privatisation as a response to digital demands in the governance of schooling. We then move on to providing an overview of the context in which New Zealand schools operate in this space, prior to explaining the ethnographic study undertaken, which draws upon data from four diverse schools and private organisations involved in their management of digital risk. Finally, we conclude with a discussion on the dangers of holding schools responsible for online safety matters and offer practical recommendations for governments and educators.

Contested educational responses to online safety: from safeguarding to critical citizenship

Over the past decade, online safety in schools has garnered significant attention in both media and academic circles worldwide. A central debate within this field has revolved around the use of restrictive measures compared to the development of educational approaches designed to enhance digital capabilities and resilience (Third et al. 2019). This debate has sparked necessary consideration of the contestability of online safety responses and underpinning positive/negative narratives about digital technology. Nevertheless, seldom has the debate ventured beyond the promotion of ‘safe’ and ‘responsible’ behaviour online (Black et al. 2022; Estellés and Doyle 2025b; Third et al. 2019) and critical notions of digital citizenship have often been overlooked (Heath 2018; Krutka, Heath, and Mason 2020, 2022). As Pangrazio and Sefton-Green (2021) note, however, the ways in which concepts such as digital citizenship and online safety are constructed matter because they shape and limit how young people (and, arguably, schools) conceptualise and engage with digital technologies.

In our previous work (Estellés and Doyle 2025b), we developed a framework that aimed to expand the range of educational responses to online safety by accounting for critical understandings of digital citizenship. This framework (Figure 1) distinguishes between four different educational approaches to online safety based on different conceptions of digital citizenship and narratives of technology: safeguarding, equipping, empowering, and resisting. Each of these approaches draws on different ontological and axiological understandings on what a ‘good’ digital citizen is, what value is attributed to digital technology, what online risk is, and how digital education should be. The horizontal axis of the model delineates between *personally responsible* notions of digital citizenship and *participatory/justice-oriented* digital citizenship (Krutka and Carpenter 2017; Westheimer and Kahne 2004), while the vertical axis represents narratives of technology based on the distinction between *techno-optimist* and *technoskeptical* used by Krutka, Metzger, and Seitz (2022). In this research, we adopt this framework as an analytical tool to examine different educational approaches to online safety in New Zealand schools. Below, we briefly explain each of these approaches.

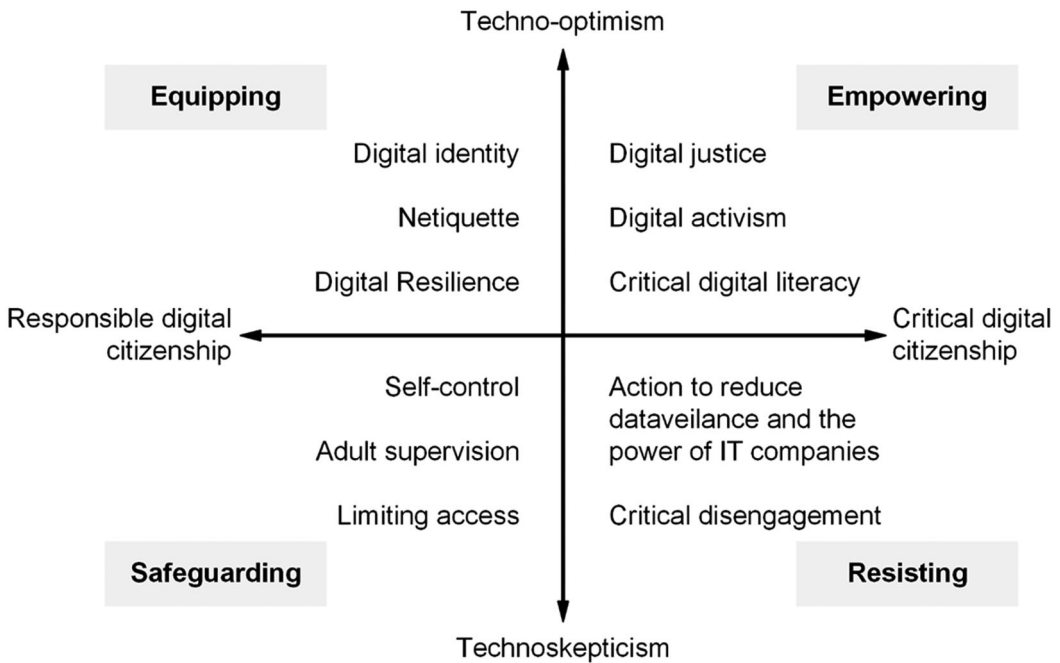


Figure 1. Educational approaches to online safety (Estellés and Doyle 2025b).

A *safeguarding* approach to online safety, often termed the ‘control paradigm’ (Third et al. 2019), is rooted in a protective framework that prioritises risk prevention over digital engagement. This approach, which became popular in the 2010s in several Anglophone countries (Johns et al. 2025), is characterised by an emphasis on the potential dangers of the digital world and aims to minimise young people’s exposure to online risks. For this approach, online threats are often related to the commonly described 3C’s risks; i.e., content, contact and conduct risks (see Staksrud and Livingstone 2009). Safeguarding measures may include content filtering, surveillance mechanisms, and restrictions on access to digital tools, all designed to limit young people’s exposure to harmful online experiences. This approach has been widely criticised in the literature for its deficit framing of young people as vulnerable populations and its consequent display of paternalistic mechanisms to minimise harm (see e.g., Black et al. 2022; Harris and Johns 2021; Third et al. 2019).

The *equipping* approach to online safety focuses on developing the knowledge and skills to navigate the digital world safely and effectively from a personally responsible citizenship perspective; i.e., someone who is law-abiding, does not harm others, volunteers, etc. (e.g., Ribble 2015; Ribble and Bailey 2007). Unlike the more restrictive safeguarding measures, this approach recognises the ubiquity and potential benefits of digital technology, emphasising that students must be prepared to engage with it responsibly rather than be shielded from it. Risk, for this approach, is conceptualised as the lack of access to digital technologies – whether in technical or capability terms – that would allow individuals to fully self-realised and be included in society. Ultimately, this approach sees digital competency as essential for both safety and success in the increasingly digitised world (Buchanan et al. 2017). This equipping approach has often been the one embraced by EdTech and pro-technology groups and has had a significant impact on education policy discourses (see Selwyn 2015; Žmavc and Bezljaj 2026).

The *empowering* approach to online safety is anchored in a critical understanding of digital citizenship that recognises how the digital has opened new possibilities for participation in social, civic and political life, but also new forms of exclusion (Pangrazio and Sefton-Green 2021). This

approach focuses on empowering students with the knowledge and skills needed to participate online and challenge social injustices perpetuated by and within digital technologies. This approach is often informed by critical pedagogies (Freire, Giroux, Apple, etc.) and views students as active agents in developing awareness of and addressing systemic inequalities. Within this approach, students may engage in critical analyses of algorithmic bias in social media and/or search engines (Pleasants et al. 2024) or may investigate how algorithms shape their online experiences and contribute to the reproduction of inequality (Benjamin 2020; Emejulu and McGregor 2019).

Finally, the *resisting* approach, as its name states, refuses to engage with digital technology. This approach is highly concerned with the commodification of personal data and wider issues of data sovereignty (Han 2017; Zuboff 2020) as it is viewed as an inherent threat/risk to personal autonomy and democracy. Social media platforms and digital services collect vast amounts of data, which leave individuals vulnerable to manipulation and surveillance. Ultimately, the resisting approach is a call for critical analysis and a conscious decision to limit engagement with digital technologies, as well as a commitment to engage in political acts that work towards the institutional enforcement of digital rights (Pangrazio and Sefton-Green 2021). While the pedagogical possibilities of this approach remain largely undertheorised, some scholars have recently begun to explore how resisting might look in the classroom (e.g., see Logan 2024).

In our previous work, we found that an overwhelming majority of the literature on online safety education has been informed by safeguarding and equipping approaches (Estellés and Doyle 2025b). For us, this dominance of safeguarding and equipping approaches is problematic because, among other reasons, both of these approaches consider the individual as the onus of change rather than, for example, governments and/or IT corporations (Estellés and Doyle 2025a). As a result of this process, which Bauman (2001) terms ‘individualisation of social risk’, teachers and schools become the primary site of contention in the debate about online safety – a pressure difficult to manage for schools.

Online safety in schools

With the spread of digital technology use, online harm has become a major concern for schools as they are often expected to manage this risk. Research on how schools respond to online harm, from early stages through to the present, highlights the use of a mixture of safeguarding and equipping measures in which restrictions and close monitoring of digital technology use are combined with the teaching of self-control and responsible use (see e.g., Martin et al. 2023; Wishart 2004). Over the last decade, the use of surveillance as a means for protecting young people has become particularly widespread, not only with students perceived as at higher risk of online harm (Caton and Landman 2022), but also as a whole school approach (Adorjan and Ricciardelli 2019). The use of this mechanism has triggered very different responses from students that range from resistance through to full support (Adorjan and Ricciardelli 2019). Research with teachers has also found that teachers are often aware of online safety issues for young people and the limitations of safeguarding approaches, but do not feel confident supporting them in managing their digital lives (Buchanan, Southgate, and Smith 2019) and have to balance this demand with other priorities (Webster 2026).

Recent literature has emphasised the importance of extending digital citizenship and young people’s rights, moving beyond a focus primarily on risk avoidance towards more empowering approaches. While in the US, Australia, and New Zealand, school-based digital citizenship education has often become closely aligned with internet safety, privacy, security, and cyberbullying, Johns et al. (2025) argue that this risk-first framing can reduce young people to vulnerable subjects in need of control and can marginalise their rights to participation, voice, cultural identity, and civic engagement. Johns et al. (2025) recognise European work with migrant and refugee youth as an alternative model, where digital citizenship and media literacy are framed more critically and participatorily, building on young people’s capabilities. A key message is the imperative to consult and

collaborate with youth about what safety and citizenship mean to them (Black et al. 2022; Castro Lopes et al. 2025), so that decisions can be made in partnership balancing young people's rights to agency, critical participation, belonging, and informed engagement (or critical disengagement) in digital society (Southgate et al. 2025). Scholars have also highlighted the tensions between young people's participatory rights and their right to privacy, since participation in the online world always involves a degree of digital surveillance, and the need for further institutional arrangements that protect young people's privacy rights without sacrificing their agency (Pangrazio and Sefton-Green 2021).

In the context of New Zealand, while research on how online safety is enacted in New Zealand schools is scarce, there have been multiple studies that have explored young people's experiences online (Classification Office 2022, 2024a; InternetNZ 2023; Netsafe 2024). These studies highlight the plethora of challenges that young people face, ranging from access to inappropriate content (InternetNZ 2023) through to the spread of misogyny culture, violent extremism (Classification Office 2024b) and sextortion (Netsafe 2024). The prevalence of online harm appears to be continually increasing. As pointed out by Netsafe in their most recent annual report, a 25% increase in HDCA complaints was received between the 2023 and 2024 financial years (Netsafe 2024).

Qualitative studies conducted by academics over the last 15 years have also identified similar trends together with the need for further support to protect young people's rights online. In their thesis investigating high school students' activity in cyber-space, for example, Fenaughty (2010) identified uncertainty among students about how to respond to challenges they encounter in cyber space, ultimately highlighting the need for interventions that assist young people in managing a range of challenges, including improving the actions they can undertake themselves, as well as increasing their ability to solicit effective support. Although exclusively focused on mobile phones, Marsh et al. (2010) found that text-based bullying was experienced by 10% of secondary school students in New Zealand – leading to students feeling unsafe in school environments, even in instances where text-based bullying occurred outside of the school environment and school hours. The two studies conducted by MacDonald-Brown and colleagues found similar trends in their analysis of the challenges that pre-teenage children face online (2016) and how they find support when risks are encountered (2017). The recurring theme that was identified in this research was the desire for more learning about digital citizenship at school (and at home). Webster's (2026) study of secondary teachers in New Zealand shows that teachers often value digital citizenship education that equips and empowers students, yet school culture, leadership priorities, and curriculum pressures continue to frequently constrain practice to centre on skills and risk management.

Policy responses and the rise of privatisation

The rise of online safety incidents at schools has triggered several responses from governmental authorities at regional and national levels. The most controversial responses have been online safety regulations, including their specific sections for the protection of children (see, for example, the UK and Australian Online Safety Acts), and the enforcement of restrictions specifically targeted to children and young people (e.g., phone bans at schools, social media bans for under 16), often promoted by international organisations (see UNESCO 2023). While these responses have been more visible in the media and public debate (see e.g., Shepherd 2025), most policy responses to online safety at schools over the last two decades have sparked little criticism and have gone more unnoticed (Estellés, Doyle, and Tan [Forthcoming](#)). These policies have often consisted of guiding frameworks and protocols for schools on how to foster online safe environments and deal with cases of online abuse and the promotion of online safety education (Frau-Meigs et al. 2017; Jang and Ko 2023). The latter often involves a broad range of initiatives, from public campaigns through to the funding of teaching resources and the inclusion of digital citizenship education in national curricula.

Over the last few years, especially after the pandemic, researchers have documented an increase in private actors providing a response to digital demands at schools (Anderson 2022; Hogan 2025; Williamson and Hogan 2020). In the space of online safety, this has led to a widespread use of digital surveillance mechanisms at schools to monitor and safeguard students (Williamson and Hogan 2020). Tools such as Gaggle Safety Management for Microsoft Teams that alert school officials when students show signs of ‘self-harm, depression, thoughts of suicide, substance abuse, cyberbullying, unhealthy relationships and credible threats of violence against others’ (Gaggle 2022) have become increasingly normalised at schools in several countries (O’Daffer, Liu, and Bloss 2025). Over the last decade, there has also been an increasing outsourcing of educational resources and programmes for ‘non-core’ curriculum areas in which teachers do not feel confident (Hogan 2025), including online safety education (Estellés, Doyle, and Fraser *Forthcoming*). These resources are often developed directly by global corporations, such as Google’s programme ‘Be Internet Awesome’, and non-profit organisations closely linked to Big Tech, such as Common-Sense Media and Media Smarts (see Estellés, Doyle, and Fraser *Forthcoming*). Additionally, several charities (e.g., Childnet), edu-businesses (e.g., Quoria) and edu-consultants (e.g., Generation Online) have emerged in this field offering more personalised solutions to schools with each of them having their own ‘niche’ market that targets different schools and demands. As Verger, Fontdevila, and Zancajo (2016) have convincingly demonstrated, the education industry, frequently catalysed and promoted by intermediary organisations such as non-government organisations and philanthropists, is very dynamic and rapidly configures new markets responding to particular demands.

The increased reliance on private organisations for the provision of education and related services has raised numerous ethical and political concerns, such as lack of transparency and accountability, agenda setting, the erosion of democratic governance at schools and the commodification of childhood (see e.g., Dormann, Hinz, and Wittmann 2019; Hogan 2025; Rönnerberg et al. 2020). The increasing privatisation of the education system, however, cannot be understood as the sole result of private actors aiming to profit from the public system (Ball 2012; Jobér 2024). As Ball (2012) explains, neoliberal practices in public schooling are the result of a ‘mutual dependency between markets and states’ (17). Public policies promoting school autonomy and decentralisation, accountability, performativity, school choice and competition have provided a breeding ground for privatisation to occur and intensify over the last few decades (Ball 2012; Hogan 2025; Verger, Fontdevila, and Zancajo 2026). For example, public schools have increasingly embraced business-like strategies in their efforts to recruit and maintain students in a competitive environment, such as engaging with specialised consultants to improve outcomes (Rönnerberg et al. 2020), using data-driven technologies for administrative efficiency (Dormann, Hinz, and Wittmann 2019) and contracting out curriculum development to create targeted interventions for specific students (Burch 2009). This quasi-market environment helps schools meet pressing demands, such as performativity, yet they have dangerous consequences for learning, equality and democracy at schools (Burch 2009; Hogan 2025). When dealing with digital pressures, the use of student digital data also raises concerns about consent, bias, privacy and ownership (Sellar and Hogan 2019). Despite all these concerns, little is known about how online safety pressures at schools might act as an ‘entry point’ for educational privatisation.

New Zealand as a case study

Over the past few decades, there has been a proliferation of private actors within and around the New Zealand education system (Thrupp et al. 2020; Wright and Peters 2017). This context was initiated by the restructuring reform of Tomorrow’s Schools within the *Education Act* (New Zealand Government 1989) that created one of the most decentralised education systems in the world (O’Neill 2011; Thrupp et al. 2020). The self-managing approach introduced by this reform together with subsequent policies that have considerably reduced the state capacity (including at a curriculum level) has opened schools up to numerous private actors to intervene in the public system (Thrupp et al. 2020).

In the online safety space, the non-profit organisation Netsafe, New Zealand's official agency, has had a main role in the provision of online safety in New Zealand schools over the last decade and, arguably, the past 25 years (Butterfield 2003). This centrality has been the result of a public-private relationship that was institutionalised with the *Harmful Digital Communications Act* (HDCA) in 2015 – an act that served as a 'very cost-efficient' response (Adams in New Zealand Parliament 2016) to the increase of crime associated with digital communications (Ministry of Justice 2015). The Act essentially absolved online content hosts from any responsibility of the harm caused by the content hosted in their platforms. As this Act mandates, Netsafe is tasked 'to provide education and advice on policies for online safety and conduct on the Internet' (Ministry of Justice 2015 Part 1, Subpart 2, S8), and the organisation offers education resources, research reports and direct assistance to schools in response to incidents. The Ministry of Education provides Netsafe with annual funding to support schools to provide online safety education, respond to incidents and advise on how 'to create a stronger overall online safety approach' (Ministry of Education, personal communication, July 25, 2024). As part of this Act, Netsafe is also required to maintain good relationships with online content hosts (HDCA 2015, 8.1.d), who are regular funders and collaborators of this non-profit that acts as an 'intermediary organisation' (Chang 2020) between Big Tech, the government and schools/individuals. This conflictive relationship has been increasingly questioned by the public, as part of broader debates about the lack of responsibility from online platforms (Espiner 2025; see also Estellés and Doyle 2025a).

Since its nomination, Netsafe has been involved in several policies to promote online safety at schools. One of the most important policies is the *Digital technology: Safe and responsible use in schools* guide aimed at supporting 'schools in the management of safe and responsible use of digital technology for learning' (Ministry of Education 2015, 1). This policy highlights a school's responsibility to provide a secure and safe learning environment and provides general advice for schools on how to prevent and respond to online safety issues. Much of this policy, despite acknowledging the limitations of safeguarding approaches and the need for equipping responses, are in turn dedicated to exploring what technical protections are feasible. For example, a highly encouraged protective measure is the use of *technology user agreements* that commit students to behave safely online and authorise schools to apply disciplinary mechanisms in the case of breaches. Since the approval of these guidelines, which are currently being reviewed (Ministry of Education, personal communication, March 13, 2025), online safety policies for schools have been more piecemeal. As part of their role, Netsafe has also been deeply involved in the development of educational resources for schools. The national curriculum does not have a clear focus on online safety or digital citizenship more generally (Webster 2024), and this curricular gap has arguably been covered by the resources and models of digital citizenship developed by Netsafe (2010, 2016, 2018). As we argue elsewhere, these resources, which have been widely promoted by the Ministry of Education (2025), advocate for a move from safeguarding to equipping approaches without fully abandoning the use of the so-called 'protective' strategies (Estellés and Doyle 2025b).

Over the years, other governmental authorities like the Department of Internal Affairs and the Prime Minister's Chief Science Advisor have also developed policies in this field, such as the public campaign *Keep It Real Online*, which aims to leave behind safeguarding strategies and move towards more equipping approaches (see Burgham 2020), and the report *He Uru Kahikatea Building Young People's Resilience through Media and Information Literacy and Digital Citizenship Skills*, whose aim is to equip individuals with 'with tools and strategies to maximise benefits and minimise harms' (Gerrard et al. 2023, 3).

Despite these policy efforts, there is growing concern in that the provision of online safety in schools is complex and insufficiently supported, with recent inquiries highlighting gaps in institutional coordination, guidance, and resourcing (New Zealand Education and Workforce Select Committee 2026). Perhaps these factors helped explain the relatively lack of resistance from the education sector to the recently introduced cell phone ban at schools (Ministry of Education 2024).

Arguably, the limited scope of these policy responses together with the neoliberal conditions in which New Zealand schools operate have left a gap for an increasing number of private actors (non-profit, for-profit, edu-consultants, etc.) to appear offering online safety services to schools. While its exact number and scope is nearly impossible to gauge, the increasing popularity of services offered by for-profit organisations such as Linewize providing digital surveillance technologies and edu-consultants and non-profits offering resources and professional development explicitly targeting New Zealand teachers (e.g., Grok Academy, Empowerment Trust NZ, Digital Waitaha, Digital Future Aotearoa, Nestconsulting, Generation Online, Learning Network, Citizen21) is a clear sign of privatisation in the field. In this study, we understand that the recent growth of private online safety providers is possibly an indicator of the need for schools to have further support in this area, as it has been the case of other educational fields affected by privatisation in the country (see e.g., Powell 2014). Yet, research is needed on how online safety is enacted in New Zealand schools to better understand the conditions enabling the spread of privatisation in this field.

Methods

Based on the theoretical framework and literature review presented, our study aimed to understand how online safety is enacted at schools, the conditions favouring the privatisation of online safety and the approaches underpinning online safety efforts (i.e., safeguarding, equipping, empowering, resisting). This study was part of a larger qualitative research project that explored how schools understand and promote safe learning environments. This article reports on the ethnographic data related to online safety, which – perhaps not surprisingly – emerged as one of the main foci of present schools’ efforts to promote safe learning environments (Estellés 2025).

Participants

The ethnographic study included four secondary schools across the country (see Table 1). With the aim of selecting schools from a broad range of circumstances, the study involved secondary schools from diverse backgrounds in terms of their size, student population (ethnicity and socioeconomic status), nature (public/state integrated and co-ed/single sex), and geographical location (urban/rural). All of the schools, however, could be considered as ‘ordinary’ (A. Braun, Maguire, and

Table 1. Overview of the schools included in the study.

Schools	Location	Nature	Size	Socio-economic status	Student demographic
School A	Large city	Public / co-ed	Large	Low	48% Pacific 19% Asian 14% NZ European 12% Māori 7% Other
School B	Large city	State integrated, single sex (girls)	Small	Low	75% Asian 19% African and Middle East 3% NZ European 2% Māori 1% Other
School C	Rural	Public / co-ed	Medium	Medium-High	64% NZ European 23% Māori 13% Other
School D	Medium size town	Public / co-ed	Medium	Medium-High	52% NZ European 16% Māori 20% Asian 4% Pacific 8% Other

Source: Based on data from the education review office.

Ball 2010) in New Zealand; that is, none of them was known for their ‘outstanding results’, ‘under performance’ or any other matter related to (online) safety. They all resorted, in one way or another, to private actors for the provision of online safety.

Data collection

The fieldwork was conducted between February 2022 and February 2024 and was structured in two phases to capture both (1) the approaches of schools and (2) the role of external actors in the provision of online safety education. This design reflects an understanding of schools as ‘complex organisations’ (Ball 2012; Lynch and Lodge 2002), while also acknowledging the developing role and place of private organisations in New Zealand schools.

The first phase focused on four secondary school sites presented in the previous section. This phase firstly, we conducted a documentary and contextual data gathering, including publicly available information (e.g., external evaluation reports, retention data, financial summaries, etc.) alongside internal school documentation such as strategic plans, vision and value statements, as well as specific policies related to online safety. Any outward-facing communications, including school newsletters and social media posts, were also gathered at this stage. These materials were, where possible, discussed with teachers and/or education leaders at the schools who helped contextualise the origins, rationale, scope and/or enactment of these policies.

The second source consisted of qualitative data generated through semi-structured interviews with school staff and focus groups with students. Across the four schools, 21 interviews and 11 focus groups were conducted (see Table 2). The interviews and focus groups centred around the ways in which safety in general and online safety in particular was understood and promoted at schools. All sessions were audio recorded and transcribed verbatim. In addition, in some interviews’ visual artefacts, such as wall displays and posters related to online safety, were discussed. These data sources were documented through photos during the school visits.

The second phase extended beyond the school sites to examine the role of external organisations in the provision of online safety education. This phase involved interviewing representatives of four

Table 2. School participants involved in the study.

School	Participant groups	<i>n</i>	Data collection methods
School A	Senior Leaders (1); Teachers (4); Teacher Aide (1); Students (7)	13	Interviews • Senior leader • Teachers • Teacher Aide Focus group • Students (2 groups)
School B	Senior Leaders (1); Teachers (3); Students (14)	18	Interviews • Senior leader • Teachers Focus group • Students (3 groups)
School C	Senior Leaders (1); Teachers (4); Teacher Aide (2); Counsellor (1); Students (23)	31	Interviews • Teachers Focus group • Senior Leader, Teacher, Counsellor • Teacher Aides • Students (4 groups)
School D	Senior Leaders (1); Teachers (4); Students (8)	13	Interviews • Senior leader • Teachers Focus group • Students (2 groups)

Table 3. Online safety providers involved in the study.

Provider	Type of organisation	Description
Netsafe	Non-profit	Independent online safety organisation. It provides support against online harm and educational programmes and services. Netsafe is the designated official agency in New Zealand to handle online safety concerns.
Linewize	For-profit	Company, part of a global digital safety technology provider named Qoria. Linewize provides digital safety tools for families, schools and districts.
Grok academy	Non-profit	Australian non-profit, online platform and professional learning provider. Grok Academy covers a range of computer education topics, including cybersecurity and digital literacy.
Individual	For-profit	Edu-consultant working with schools and other sectors and providing advice on online safety.

online safety education providers that were mentioned by participants from schools. These organisations operated independently of the schools and included a mix of for-profit and non-profit providers (Table 3). Semi-structured interviews were conducted with one representative from each organisation. These interviews focused on the nature of their work with schools, the challenges they encountered, the feedback they received from educators and students, their organisational histories, and their sources of funding. Conducted online, these interviews provided insight into the broader policy and provision landscape within which schools are situated, and the ways in which external actors contribute to shaping understandings and practices of online safety.

Data analysis

For the data analysis, we used a ‘thematic analysis’ (V. Braun and Clarke 2022). The coding and theme development involved in this process was informed by two main theoretical resources. On the one hand, it was drawn on our previously explained framework (see Figure 1), which provided us with a range of questions to *deductively* guide the thematic analysis such as: what is considered safe in the online world? what is seen as dangerous? How is digital technology portrayed? How are ‘good digital citizens’ portrayed? And which solutions to online risk are put forth? The data analysis was also informed by the work of sociologists of education on privatisation at schools (Ball 2012; Hogan 2025), including New Zealand schools (O’Neill 2011; Powell 2014; Thrupp et al. 2020) and, in particular, the conditions that have influenced the rise of private actors in the online safety

Table 4. Coding framework: Subthemes and themes.

Codes or subthemes	Themes
Recurrence and gravity of online safety issues	Online safety: A significant issue for schools
Risk/harm as 3C’s	
Digital technologies as dangerous weapons	
Digital citizenship as responsible and safe behaviour	Difficult for schools to manage
Digital harms as violations of rights	
Outside of school hours	
Social media sites are not responsive	
School competition environment and school reputation	Dominance of safeguarding measures
Incident management pressures	
Technology use agreements	
Filters and access restrictions	
Behavioural protocols	
Phone bans	Online safety education: a de facto curricular gap
Teaching of self-safeguarding strategies	
Time restrictions	
Overloaded curriculum	
External examinations	Outsourcing the curriculum
Little attention to online safety education	
Resources from private organisations or public campaigns	External online safety solutions
Equipping approaches	
Techno-solutions	
External specialised actors	

field. The combination of these two theoretical frameworks in the thematic analysis resulted in the development of the six themes presented in the findings section (see [Table 4](#)).

Funding and ethics

The research project was funded by the Spencer Foundation (#202200161) with further support from the Division of Education at the University of Waikato (#110448) to conduct the fourth phase of the study with online safety providers. The research had the ethical approval of the University of Auckland and the University of Waikato where the study was conducted.

Findings

Online safety: a significant issue for schools

In alignment with national (Classification Office [2024a](#)) and international literature (e.g., United Nations [2021](#)), our conversations with the participants highlighted that online harm is a significant issue for young people nowadays. Online harm was usually understood as that related to the 3C's of online safety (i.e., content, contact, conduct) with issues of cyberbullying, sensitive content sharing and harassment being the most cited. As the following teacher and students' voices expressed:

Digital safety stuff is horrific ... there's some terrible bullying, you know, sharing of nudes and stuff like that, which is, yeah, it's mind blowing (Teacher, School D)

Online safety stuff is huge at the moment ... Literally just night, I got a DM by just a random stranger being like, hey, how old are you? ... I feel it happens quickly very often (Student, School C)

Online safety issues related to online conduct and content sharing were also affecting educators at schools. Indeed, several teachers across the four schools referred to online devices as 'dangerous weapons'. In their interviews, teachers denounced the conduct and content risks that they were increasingly exposed to with digital technologies. See, for example, the following case explained by a senior leader:

We had one teacher, a younger female teacher, accused on here to have sent nudes around the internet. And of course, it wasn't true. But it was deeply distressing to that teacher and potentially career ending (Senior leader, School C)

The online harms mentioned by the teachers and students sometimes took place at schools, sometimes outside. Yet the boundaries between both worlds were blurry, as literature on the postdigital has convincingly argued (Jandrić and Knox [2022](#); Knox [2022](#)). While harm might start in a personal context, it can easily spill over into the school environment and vice versa. As an example, one of the teachers explained how she had several students who did not want to go to the school toilets to avoid being recorded:

I have had lots of kids say that they can't go to the toilet ... because when they go in there, there's too many kids. They're all in here. They feel intimidated. They are scared of being recorded. So they wait when they go home (Teacher, School C)

As previous research on school violence has repeatedly pointed (e.g., Meyer [2015](#)), our study also found that students from historically discriminated/oppressed groups were more prone to be the target of online abuse, particularly female students. As an example, cases of female students' private photos being 'leaked and sent around', as a teacher put it (School A), were common in all schools. These inequalities, however, were not portrayed by any participant as an 'online risk'.

Dataveillance or violations of privacy rights were not considered as online risks by the school participants. Indeed, as will be shown in the following sections, monitoring students' online activity was a common practice at all schools.

Difficult for schools to manage

One of the recurrent themes identified was that online safety issues at schools are difficult to manage. They often involve violations of rights, which may or may not take place on school grounds or within school hours. Senior leaders of all schools acknowledged being overwhelmed with the number of cases they had to deal with, as previous studies with principals have indicated (Dunsmore 2021). Put simply, online safety issues are too significant a problem for schools to handle on their own. The following teacher expressed some of these difficulties:

It's a tricky one because you've got things that are taking place outside of the school, but they relate to people within the school. But because it's taking place outside the school, there's only a certain element the schools can do (Teacher, School A)

Perhaps the biggest difficulty lies in the fact that online safety issues are not easily prevented. In the words of the Netsafe representative, 'nobody yet knows what the magic button is to prevent the harm'. Safeguarding measures, although perceived as helpful by most participants, are often not as effective as envisioned. As explained by both teachers and students, there are several ways in which students override these measures:

the school tries to block off certain social media apps, but there's a VPN thing, an app you download, where you can use the school WiFi while ... so there's no point (Student, School A)

Once an incident of online abuse has happened, removing the harmful online content is not an easy task either. Social media platforms are not very responsive to the schools' demands for online safety. They only respond to Netsafe's calls. As explained by the following senior leader:

Netsafe were really good. At the first call, they got it [fake profile] shut down really quickly. I initially went directly to Instagram, but after a couple of weeks they said it wasn't applicable for me to make the complaint because I wasn't the one affected, they needed the victim to contact. So Netsafe did all that. I found Instagram to be really slow and non-responsive ... Netsafe said I will make that phone call for you. And they did it in a couple of days versus me trying to fight for ... (Senior Leader, School C)

Another challenge posed by online safety issues at schools was the risk of damaging their public image in a context of school competition. The fear of harming the school reputation (with all the associated consequences over student retention and recruitment and, eventually, funding) put principals in a situation of needing to be extra-vigilant of all the content posted online related to the schools, as previously noted by Dunsmore (2021). As explained by the following associate principal, a substantial part of his job has become to chase fake social media profiles attempting to damage the school's reputation:

A big part of my job is to [put down] groups that have set up outside of school time, outside of school networks, often anonymously ... using variations of the name of the school and they just post horrendous, toxic, really quite gruesome, nonsense ... I think I'm up-19 of those pages because you put one down, we call it away. Come on, you get one shot down. Another one extra dot and the name would pop up in a different set of stuff or sometimes the same stuff (Senior Leader, School C)

Concerns over how a school's image or 'brand' is presented on social media required time and efforts to manage. As noted by the Netsafe representative, this effort often even becomes the priority:

we're aware that lots of schools will love us, but they will love us because we're a cloak of protection. Not necessarily because we're helping them to appropriately address the issues ... I'm always like, but is that because you think this was the right thing to prevent and remediate harm? Or is it because when something goes wrong and you're in the media, you can say we're working with Netsafe, and that gives you some kind of brand protection?

Dominance of safeguarding measures

All schools included in the study primarily used safeguarding measures to deal with online safety issues, although these sometimes required the use of (arguably, limited) equipping strategies. As

part of the centrally administrated Network for Learning (N4L) facilitated by the Ministry, each school used filters to restrict access to ‘dangerous’ or ‘potentially harmful’ sites (again, understood from the 3C’s perspective) under the schools’ network and devices. These access restrictions often included social media sites. Another common practice in all schools was the signing of the previously mentioned technology user agreements, which were used by schools as a means to both raise awareness about the need to behave safely online (equipping) and authorise schools to monitor the use of technology and penalise inappropriate usage (safeguarding). As explained by a senior leader:

Our Technology User Agreement, parents and students have to sign it [...] And if they sign it, it means that they understand what we see as the safe use of technology in our school. And if they do misuse it, then there are consequences in place that could happen. And we’ve done that before, a few times when we’ve had a misuse of technology, they’re not allowed to use it for the rest of the term or two weeks or depending on whatever the case is (Senior leader, School B)

While these user agreements are framed as an act of coming to a mutual arrangement, there is no discussion or ability to reject involved – everyone at school must sign it.

Two of the schools included in the study (School B and D) also banned the use of phones, unless they were used in class for teaching and learning purposes (please note that this research was conducted prior to this measure being enforced nationally in 2024). This safeguarding strategy came together with control mechanisms to make sure this policy was being complied with. As explained by the following teacher:

when students arrive to class, a cell phone is meant to be put into a box, or controlled in some way. So then, that digital space is then under the teacher’s control (Teacher, School C).

The teaching of safeguarding strategies, such as blocking, screenshotting or reporting cases of online abuse to Netsafe, was also a measure used by the schools to help them release the burden of dealing with high numbers of online abuse. As explained by a senior leader:

So we’ve been quite proactive ... A lot of students now have the techniques, the strategies of blocking, screenshotting, referring to police if it’s getting worse. So we’re receiving less reports of social media, safety concerns and abuse ... probably because they are now reporting it to higher authorities (Senior Leader, School C)

Online safety education: a de facto curricular gap

Most students across the four schools recognised not having had many opportunities for online safety education. Commentaries like the following were common in the focus groups:

[To the question: Have you ever received any education around OS?]

Student 1: I think we have. But I think we’re a bit younger. Yeah. I can’t remember.

Student 2: Yeah, I know we’ve done it in Health, especially in Year 9 and 10, like a little bit. Not a lot.

Many of the students criticised the safeguarding measures adopted by the schools (phone bans, site blocking, etc.), particularly when such measures did not consider any ‘equipping’ approaches that would teach them how to navigate the online world in an ethical and safe (i.e., personally responsible) manner. As one student highlighted:

I feel like we shouldn’t, instead of just blocking sites from school, we should teach students how to use those sites right. Because the thing is, you can block the sites at school, but then they still all of this going on at home ... And I feel like instead of just being like, don’t use the site, don’t do anything like near it. It’s better to teach them how to use it wisely (Student, School B)

The limited attention to online safety education was also noted by teachers across the four schools. With a sense of guilt, some teachers recognised that they should be working more in this space. Yet, they also raised concerns about time restrictions, overloaded curricula and the focus on external examinations. As the following social studies teacher explained:

Honestly, I'd love to talk more about these things with the kids, I think this is something they really need to learn about because the consequences are so massive, but at the same time, when? We have NCEA [external evaluations] around the corner ... I feel I am constantly in a rush. I want to think they look at it in other [subjects] (Teacher, School C)

The fact that online safety education is not explicitly addressed in the curriculum leaves the door open for no one to explicitly teach it. In the schools involved in the study, this responsibility was often taken by the health teachers and/or head teachers, although occasionally counsellors also stepped in with equipping approaches once the abuse had already happened. See for example:

The victim [of cyberbullying] is somebody that you've got to work with very, very carefully, because it's all around their emotions have been hurt, and you can't take back what was posted. But you can teach resilience, you can teach how to work through that. So we work through that situation ... How do you build that resilience (Counsellor, School C)

Outsourcing curriculum

In class, most teachers used external ('ready-to-use') resources, often developed by private, non-profit organisations (i.e., Netsafe, Grok Academy), to teach about online safety, usually under safeguarding and equipping approaches. As a head teacher explained:

In some cases, we'll do one lesson on phone safety with Netsafe videos about people discussing these matters, and how quickly they can escalate as well ... But we don't go into much depth (Teacher, School D)

The public campaign Keep It Real was also a resource used by some teachers. The students appreciated the entertaining component of this resource, yet recognise that there was not much more engagement with the topic beyond the watching of this TV show:

They [teachers] showed us the Eggplant. Yeah. That was the most fun. Like a phone safety campaign ... all for online safety. And I was like a little TV show. And I remember people were excited to watch it, even though it had the whole theme. And the overarching message was about the dangers of social media and how to deal with it. It was cool but I can't remember doing much more than that (Student)

One of the teachers involved in the study opted for a gamified resource developed by Grok Academy. As this teacher described, he selected this resource for engaging students in 'real life situations in a fun way'. Beyond these pedagogical considerations, however, none of the school participants questioned the approach of online safety adopted by these resources/organisations and none of them showed signs of using empowering and resisting approaches. This could be attributed to the lack of public debate around these educational options (Estellés and Doyle 2025a) and to the tendency for whatever professional development was available to be offered by the same providers:

Have you received any PD on online safety? ... A couple of years ago we had to do a Netsafe thing one week. Yeah, Netsafe came in and talk to us (Teacher)

Resorting to external solutions

When online safety issues arise at schools, a common strategy used by the participant schools was the use of external providers. Netsafe and the Police were the most common external providers mentioned by the school participants. The former frequently acted as a liaison between social media platforms and schools in the blocking of online harmful content. The latter was usually called upon to deal with serious cases. This external service was highly appreciated by schools:

The police were very good, the police were very prompt. And they got well got our view in which I had a record of all the incidences that had occurred between the two students. And the police were very quite responsive. They came in had a meeting with the students. And they kind of approached it as an educational

process, that educational stance, this is the issue. This is how it's affecting you and the person that you are messaging and it needs to stop now. So as a strong warning (Senior leader, School D)

For-profit organisations were also offering technosolutions to online safety issues at schools. For example, Family Zone (now Linewize) was used by the state-integrated school involved in the study. The rationale for resorting to this private solution was explained by the senior leader of this school in the following quote, where the safeguarding nature of this technosolution and the lack of concern around students' privacy rights are also present:

We've got recently got Family Zone. So that's an external provider. What they do is they help us monitor students searches, and their uses on their devices. So our pastoral care head and myself, we get notifications of the red flags coming up. So for example, if students are searching for adult content or something inappropriate, then we get the red alert ... It's just gives a notification to the student that was trying to go into there, then we have that conversation again with the kid: 'I see that you were going on this website, what's happening?, What were you searching for?' ... And most of the times, they are good, you know, but we did have a student who gave us a suicide red alert. She searched up for something to do with suicide and that caused a red flag instantly. So we moved to refer her instantly to the counsellor (Senior Leader, School B).

Discussion and implications

Aligned with recent reports on young people's online experiences (e.g., Classification Office 2024a), our study shows that online harm is a significant issue for young people and points at several instances indicating violations to their rights. These include their right to be protected from violence and abuse (art. 19 of the United Nations Convention on the Rights of the Child), to privacy (art. 16), to be protected from sexual abuse (art. 34) and even to be treated fairly (art. 2), as some groups, particularly female students, seemed to be more affected than others. As the findings show, these online safety issues present pressing management problems for schools, which often escape their control as online abuse can take place outside of the school and the impact extends beyond its walls. The expectation for schools to provide safe environments for students without demanding further responsibilities from governments and online platforms seems unrealistic, as public agencies are also recognising (Department of Internal Affairs 2024). To the pressure of protecting students from online harm, schools also had the added pressure of maintaining their reputation, as cases of online abuse could significantly impact student numbers (and, therefore, funding) – a situation arguably a result of the self-managing model of New Zealand schools (see Wylie 2012).

The schools involved in this study managed the (arguably, unrealistic) expectation of online safety by predominantly using safeguarding approaches that restricted and closely supervised the use of digital technologies, sometimes at the expense of young people's privacy rights. In addition, the schools made use of some equipping strategies aimed at teaching students how to safely navigate the online world, yet these were limited. This limited attention to online safety education seemed to be the result of several circumstances, including overloaded teachers, narrowed curriculum, limited curricular emphasis on online safety, and lack of professional development. These circumstances, together with the pressures mentioned above, opened the door for private actors to offer their services, and in turn, setting the agendas of online safety at schools. This process of privatisation has been similar to that experienced by other curriculum learning areas in the New Zealand education system (see Thrupp et al. 2020). While the agendas of the private actors are diverse, they all restrict the debate on online safety education to either safeguarding or equipping approaches (Estellés and Doyle 2025b) and, therefore, portray online safety as a matter of individual responsibility. This form of 'individualisation of social risk' (Bauman 2001) is problematic because it prevents students from understanding the role of governments and IT corporations in their digital experiences and, therefore, from demanding political responses from them.

In summary, our study suggests that the privatisation of public education that is taking place via online safety services is the product of a combination of the pressure and significance of online safety issues *together with* the conditions of self-management, accountability and competition in

which schools operate. Our study has also found that private actors are not only providing a limited response to the complex question of youth online safety, but also are creating additional ethical and political issues, including the violation of young people's privacy rights and the spread of individualising narratives of digital citizenship that overlook institutional responses. These findings have important implications for governments and educators at different levels. At governmental level, this study indicates that schools cannot carry by themselves (or together with parents) the burden of protecting young people's safety online; further accountability and statutory duty of care from online platforms is needed, as several voices have recently pointed (Espiner 2025; Tan 2022). A recent sign of a shift towards design-based accountability is the 2026 California jury verdict against Meta and Google/YouTube, which found the companies liable in a landmark social media addiction trial. The case is significant because it frames youth harm not only in terms of exposure to risky content, but in relation to addictive platform features and failures to warn, reinforcing wider scholarly arguments that children's rights online are shaped by platform architecture as well as user behaviour (Humphry et al. 2026; Nash and Felton 2024). Furthermore, a core issue is not only exposure to harm online but also the opaque collection, profiling, monetisation, and governance of young people's data (Southgate et al. 2025). Under New Zealand legislation, the responsibility of protecting young people from online harm falls exclusively under the remit of individual schools, teachers and parents, and there is not enough institutional investment in the effective enactment of the Privacy Act (Privacy Foundation NZ 2022). Yet, this self-regulated model is clearly not enough in light of this and other studies (Classification Office 2022, 2024a; InternetNZ 2023; Netsafe 2024; Wiggins 2020).

At an education system level, there are several systemic issues that hinder an adequate response. First, the self-managing model of the New Zealand education system, under considerable underfunding conditions, places so many responsibilities on individual schools, including the competition for resources, that are already overloaded (Tomorrow's Schools Independent Taskforce 2019). As shown above, this situation clearly comprises the commitment to putting children's rights at the centre. Increasing the public funding of the education system and the introduction of regional boards, as recommended by the Independent Taskforce (2019) that reviewed the Tomorrow Schools reform, is necessary to release the pressure from the system and prioritise young people's rights. Second, the lack of a clear curricular emphasis on digital citizenship at a national level (Webster 2024) – and little signs of follow-up from the Education Review Office – contributes to relegate this crucial area to the margins of the school curricula.

Third, our study also indicates the need to articulate more critical online safety responses. It is imperative to develop resources that venture beyond safeguarding and equipping approaches, to support school leaders, teachers and students with critical digital citizenship and recognise the possibility to resist via critical disengagement. Such resources could inform projects that engage students with critical questions such as: Who controls and designs digital technologies?, Under which drivers and values?, How do digital technologies impact our lives and societies?, How are the benefits/drawbacks of digital technologies distributed across different social groups? and How can citizens use legislation and other political means to make online environments more democratic and safe? These resources could be developed together with students, be contextualised around online safety issues that matter to them and promote a sense of agency that enables them to further exercise their participatory rights. At the moment, however, most digital citizenship and online safety resources adopted at a scale globally are developed by non-profit organisations closely connected to Big Tech and, therefore, have a strong focus on equipping/individual approaches (see Estellés, Doyle, and Fraser [Forthcoming](#))

Fourth and finally, our study also highlighted the need for further professional learning and development in this area. Professional learning cannot be reduced to a presentation at a staff meeting (Forbes and Walker 2022). It must also engage with critical digital citizenship questions such as the ones mentioned above, which is unlikely to happen when professional learning providers are not independent from the IT industry.

To conclude, the protection of young people's rights in the online world is a pressing concern for schools. This crucial endeavour, however, cannot be solely left to schools and does not have a quick, easy fix. While private actors present themselves as the best solution to this problem, they provide limited and problematic responses. Addressing online safety requires more critical and comprehensive approaches.

Acknowledgements

We would like to thank the two anonymous reviewers for their thoughtful and constructive feedback, which we feel has strengthened the manuscript.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Spencer Foundation under grant #202200161; and the Division of Education, The University of Waikato under grant number #110448.

ORCID

Andrew Doyle  <http://orcid.org/0000-0003-1993-683X>

Marta Estellés  <http://orcid.org/0000-0001-6162-3875>

Dianne Forbes  <http://orcid.org/0000-0001-6557-5305>

References

- Adorjan, M., and R. Ricciardelli. 2019. "Youth Responses to the Surveillance School: The Bifurcation of Antagonism and Confidence in Surveillance among Teenaged Students." *Young* 27 (5): 451–467. <https://doi.org/10.1177/1103308818821206>.
- Anderson, M.. 2022. *Public Education in the Digital Age: Neoliberalism, EdTech, and the Future of Our Schools*. 1st ed.. New York: Routledge. <https://doi.org/10.4324/9781003344308>.
- Ball, S. J.. 2012. *Global Education Inc.: New Policy Networks and the Neoliberal Imaginary*. London: Routledge. <https://doi.org/10.4324/9780203803301>.
- Ball, S. J., and D. Youdell. 2008. *Hidden Privatisation in Public Education*. Education International. <https://www.ei-ie.org/en/item/25671:hidden-privatisation-in-public-education>.
- Bauman, Z.. 2001. *The Individualized Society*. Cambridge: Polity Press.
- Benjamin, R.. 2020. *Race after Technology*. Cambridge: Polity.
- Black, R., L. Walsh, C. Waite, P. Collin, A. Third, and S. Idriss. 2022. "In Their Own Words: 41 Stories of Young People's Digital Citizenship." *Learning, Media and Technology* 47 (4): 524–536. <https://doi.org/10.1080/17439884.2022.2044848>.
- Braun, A., M. Maguire, and S. J. Ball. 2010. "Policy Enactments in the UK Secondary School: Examining Policy, Practice and School Positioning." *Journal of Education Policy* 25 (4): 547–560. <https://doi.org/10.1080/02680931003698544>.
- Braun, V., and V. Clarke. 2022. *Thematic Analysis: A Practical Guide*. London: SAGE.
- Buchanan, R., E. Southgate, and S. P. Smith. 2019. "'The Whole World's Watching Really': Parental and Educator Perspectives on Managing Children's Digital Lives." *Global Studies of Childhood* 9 (2): 167–180. <https://doi.org/10.1177/2043610619846351>.
- Buchanan, R., E. Southgate, S. P. Smith, T. Murray, and B. Noble. 2017. "Post No Photos, Leave No Trace: Children's Digital Footprint Management Strategies." *E-Learning and Digital Media* 14 (5): 275–290. <https://doi.org/10.1177/2042753017751711>.
- Burch, P.. 2009. *Hidden Markets: The New Education Privatization*. 1st ed.. New York: Routledge. <https://doi.org/10.4324/9780203883945>.
- Burgham, L. 2020. "Keep it Real Online: The Story Behind NZ's Viral Internet Safety Campaign." *The New Zealand Herald*. <https://www.nzherald.co.nz/lifestyle/keep-it-real-online-the-story-behind-nzs-viral-internet-safety-campaign/TX6HLZU4INM2DRPVPVMLDIFOII/>.

- Butterfield, L. 2003. "NetSafe: The New Zealand Model for Internet (ICT) Safety Education." <https://community.isc2.org/ijoyk78323/attachments/ijoyk78323/industry-news/5927/1/10.1.1.394.3427.pdf>.
- Castro Lopes, S., L. Holly, and I. Kickbusch. "Mapping Policies and Regulations for Safe and Healthy Digital Environments for Children and Adolescents." *Global Policy* 16 (2): 380–384. <https://doi.org/10.1111/1758-5899.13492>.
- Caton, S., and R. Landman. 2022. "Internet Safety, Online Radicalisation and Young People with Learning Disabilities." *British Journal of Learning Disabilities* 50 (1): 88–97. <https://doi.org/10.1111/bld.12372>.
- Chang, E. 2020. "Digital Meritocracy: Intermediary Organizations and the Construction of Policy Knowledge." *Educational Policy* 34 (5): 760–784. <https://doi.org/10.1177/0895904818802116>.
- Classification Office. 2022. *What We're Watching: New Zealanders' Views about What We See on Screen and Online*. Te Mana Whakaatu Classification Office. <https://www.classificationoffice.govt.nz/resources/research/What-Were-watching/>.
- Classification Office. 2024a. *On Our Screens – 2024 Survey Snapshot*. Classification Office. <https://www.classificationoffice.govt.nz/resources/research/on-Our-screens-survey-snapshot/>.
- Classification Office. 2024b. *Online Misogyny and Violent Extremism: Understanding the Landscape*. Classification Office. <https://www.classificationoffice.govt.nz/resources/research/online-misogyny-and-violent-extremism-summary-report/>.
- Department of Internal Affairs. 2024. Proactive Release of Public Submissions Organisations – Part A (Safer Online Services and Media Platforms). Wellington: Department of Internal Affairs. [https://www.dia.govt.nz/diawebsite.nsf/Files/online-content-regulation/\\$file/Organisations-Part-A.pdf](https://www.dia.govt.nz/diawebsite.nsf/Files/online-content-regulation/$file/Organisations-Part-A.pdf).
- Dormann, M., S. Hinz, and E. Wittmann. 2019. "Improving School Administration through Information Technology? How Digitalisation Changes the Bureaucratic Features of Public School Administration." *Educational Management Administration & Leadership* 47 (2): 275–290. <https://doi.org/10.1177/1741143217732793>.
- Dudman, S. 2021. *Whanganui Police Step in as Kids 'Assaulted' in Social Media Craze*. Whanganui Chronicle, April 16. <https://www.nzherald.co.nz/nz/whanganui-police-step-in-as-kids-assaulted-in-social-media-craze/D2D4ANTXZ34IO6UUI6RL2MD63E/>.
- Dunsmore, S. 2021. "Principals' Experience of Social Media in New Zealand Schools." Master's thesis, University of Waikato. <https://hdl.handle.net/10289/14453>.
- Emejulu, A., and C. McGregor. 2019. "Towards a Radical Digital Citizenship in Digital Education." *Critical Studies in Education* 60 (1): 131–147. <https://doi.org/10.1080/17508487.2016.1234494>.
- Espiner, G. 2025. "Netsafe's Tech Ties Spark Calls for Independent Regulator." RNZ. <https://www.rnz.co.nz/news/in-depth/542415/netsafe-s-tech-ties-spark-calls-for-independent-regulator>.
- Estellés, M.. 2025. *The Safetyfication of Education: Neoliberalism, Psychopolitics and the End of Critical Education*. 1st ed.. London: Bloomsbury Academic. <https://doi.org/10.5040/9781350533950>.
- Estellés, M., and A. Doyle. 2025a. "Educating Digital Citizens at Risk: Private Actors, Neoliberal Policies, and Individualising Narratives." In *Postdigital Education for Development*, edited by M. A. Peters, O. Kamenarac, B. J. Green, P. Jandrić, and T. Besley, 137–160. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-99247-6_7.
- Estellés, M., and A. Doyle. 2025b. "From Safeguarding to Critical Digital Citizenship? A Systematic Review of Approaches to Online Safety Education." *Review of Education* 13 (1): e70056. <https://doi.org/10.1002/rev.3.70056>.
- Estellés, M., A. Doyle, and Z. Fraser. *Forthcoming*. "Who Teaches Digital Citizenship? Private Actors, Educational Resources and Individualising Discourses." *Social Sciences*.
- Estellés, M., A. Doyle, and R. Tan. *Forthcoming*. "Embracing Co-Governance: The Policies and Politics of Online Safety Education." *Journal of Education Policy*.
- Fenaughty, J. 2010. "Challenging Risk: NZ High-School Students' Activity, Challenge, Distress, and Resiliency, within Cyberspace." PhD diss. <https://researchspace.auckland.ac.nz/handle/2292/6775>.
- Forbes, D., and R. Walker. 2022. *Developing Online Teaching in Higher Education: Global Perspectives on Continuing Professional Learning and Development*. Singapore: Springer Nature. <https://doi.org/10.1007/978-981-19-5587-7>.
- Frau-Meigs, D., B. O'Neill, A. Soriani, and V. Tomé. 2017. *Digital Citizenship Education: Overview and New Perspectives*. Strasbourg: Council of Europe. <https://rm.coe.int/prems-187117-gbr-2511-digital-citizenship-literature-review-8432-web-1/168077bc6a>.
- Gaggle. 2022. "The Gaggle Safety Team: The Heart of Student Safety." Gaggle. <https://www.gaggle.net/blog/the-gaggle-safety-team-the-heart-of-student-safety>.
- Gerrard, J., S. McNaughton, M. Webber, C. Verdonk, and S. Meade. 2023. *He Uru Kahikatea Building Young People's Resilience through Media and Information Literacy and Digital Citizenship Skills: A Report from the Prime Minister's Chief Science Advisor, Kaitohutohu Mātanga Pūtaiao Matua ki te Pirimia*. Office of the Prime Minister's Chief Science Advisor. <https://www.pmcsa.ac.nz/topics/building-young-peoples-resilience-through-media-and-information-literacy-and-digital-citizenship/>.
- Han, B.-C.. 2017. *In the Swarm: Digital Prospects*. Cambridge: MIT Press.

- Harris, A., and A. Johns. 2021. "Youth, Social Cohesion and Digital Life: From Risk and Resilience to a Global Digital Citizenship Approach." *Journal of Sociology* 57 (2): 394–411. <https://doi.org/10.1177/1440783320919173>.
- Harmful Digital Communications Act 2015. 2015. No. 63. Wellington: New Zealand Government. <https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html>.
- Heath, M. K. 2018. "What Kind of (Digital) Citizen? A Between-Studies Analysis of Research and Teaching for Democracy." *The International Journal of Information and Learning Technology* 35 (5): 342–356. <https://doi.org/10.1108/IJILT-06-2018-0067>.
- Hogan, A. 2025. *Commercialising Public Schooling: Practices of Profit-Making*. 1st ed.. Abingdon: Routledge. <https://doi.org/10.4324/9781003213093>.
- Humphry, J., J. Hutchinson, and O. Boichak. 2026. "Social Digital Dilemmas: Young People's and Parents' Negotiation of Emerging Online Safety Issues." *New Media & Society* 28 (3): 1274–1294. <https://doi.org/10.1177/14614448241310247>.
- InternetNZ. 2023. *New Zealand's Internet Insights 2023: A Verian Research Report*. <https://internetnz.nz/new-zealands-internet-insights/new-zealands-internet-insights-2023/>.
- Jandrić, P., and J. Knox. 2022. "The Postdigital Turn: Philosophy, Education, Research." *Policy Futures in Education* 20 (7): 780–795. <https://doi.org/10.1177/14782103211062713>.
- Jang, Y., and B. Ko. 2023. "Online Safety for Children and Youth under the 4Cs Framework – A Focus on Digital Policies in Australia, Canada, and the UK." *Children* 10 (8): 1415. <https://doi.org/10.3390/children10081415>.
- Jobér, A. 2024. "Private Actors in Policy Processes. Entrepreneurs, Edupreneurs and Policyneurs." *Journal of Education Policy* 39 (1): 20–39. <https://doi.org/10.1080/02680939.2023.2166128>.
- Johns, A., A. Harris, E. Booth, G. Caluya, and J. Walton. 2025. "Beyond Risk: Reducing the Gap between Diaspora Youth Digital Citizenship Needs and School Curricula." *Learning, Media and Technology* 1–15. <https://doi.org/10.1080/17439884.2024.2448549>.
- Knox, J. 2022. "Educational Development in the Postdigital Era." In *International Handbook on Education Development in Asia-Pacific*, edited by W. O. Lee, P. Brown, A. L. Goodwin, and A. Green, 1–20. Singapore: Springer Nature. https://doi.org/10.1007/978-981-16-2327-1_119-1.
- Krutka, D. G., and J. P. Carpenter. 2017. "Digital Citizenship in the Curriculum: Educators Can Support Strong Visions of Citizenship by Teaching with and about Social Media." *Educational Leadership* 75 (3): 50–55.
- Krutka, D. G., M. K. Heath, and L. E. Mason. 2020. "Editorial: Technology Won't Save Us – A Call for Technoskepticism in Social Studies." *Contemporary Issues in Technology and Teacher Education* 20 (1): 108–120.
- Krutka, D. G., S. A. Metzger, and R. Z. Seitz. 2022. "Technology Inevitably Involves Trade-Offs": The Framing of Technology in Social Studies Standards." *Theory & Research in Social Education* 50 (2): 226–254. <https://doi.org/10.1080/00933104.2022.2042444>.
- Logan, C. 2024. "Learning about and against Generative AI through Mapping Generative AI's Ecologies and Developing a Luddite Praxis". *Proceedings of the International Conference of the Learning Sciences* 362–369. <https://doi.org/10.22318/icls2024.259570>.
- Lynch, K., and A. Lodge. 2002. *Equality and Power in Schools: Redistribution, Recognition and Representation*. London: RoutledgeFalmer.
- Marsh, L., R. McGee, S. Nada-Raja, and S. Williams. 2010. "Brief Report: Text Bullying and Traditional Bullying among New Zealand Secondary School Students." *Journal of Adolescence* 33 (1): 237–240. <https://doi.org/10.1016/j.adolescence.2009.06.001>.
- Martin, F., J. Bacak, D. Polly, W. Wang, and L. Ahlgrim-Delzell. 2023. "Teacher and School Concerns and Actions on Elementary School Children Digital Safety." *TechTrends* 67 (3): 561–571. <https://doi.org/10.1007/s11528-022-00803-z>.
- Meyer, E. J. 2015. *Gender, Bullying, and Harassment: Strategies to End Sexism and Homophobia in Schools*. 2nd ed.. New York: Teachers College Press.
- Ministry of Education. 2015. *Digital Technology: Safe and Responsible use in Schools*. <http://www.education.govt.nz/assets/Documents/School/Managing-and-supportingstudents/DigitalTechnologySafeAndResponsibleUseInSchs.pdf>.
- Ministry of Education. 2024. "Phones Away for the Day – Education in New Zealand". <https://www.education.govt.nz/school/digital-technology/cellphones/>.
- Ministry of Education. 2025. "Digital Citizenship Modules." Tāhūrangi – New Zealand curriculum. <https://newzealandcurriculum.tahurangi.education.govt.nz/digital-citizenship-modules/5637209137.p>.
- Ministry of Justice. 2015. "Harmful Digital Communications Act – HDCA." Ministry of Justice. <https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html>.
- Netsafe. 2010. *Digital Citizenship in New Zealand Schools: Overview*. Netsafe. https://www.Netsafe.org.nz/wpcontent/uploads/2015/09/Digital_Citizenship_in_New_Zealand_Schools_Overview.pdf.
- Netsafe. 2016. *From Literacy to Fluency to Citizenship: Digital Citizenship in Education*. Netsafe. <https://www.netsafe.org.nz/wp-content/uploads/2016/11/NETSAFE-WHITEPAPERFrom-literacy-to-fluency-to-citizenship.pdf>.
- Netsafe. 2018. *From Literacy to Fluency to Citizenship: Digital Citizenship in Education*, 2nd ed. NetSafe. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3220745.

- Netsafe. 2024. *Year in Review: July 2023–June 2024*. Netsafe. <https://netsafe.org.nz/our-work/reports-and-research>.
- New Zealand Education and Workforce Select Committee. 2026. "Inquiry into the Harm Young New Zealanders Encounter Online, and the Roles that Government, Business, and Society Should Play in Addressing those Harms." New Zealand Parliament. <https://selectcommittees.parliament.nz>.
- New Zealand Government. 1989. *Education Act*.
- New Zealand Parliament. 2016. *Parliamentary Debates (Hansard) Budget Debate, 714*. Accessed November 21, 2025. https://www.parliament.nz/en/pb/hansard-debates/rhr/document/51HansD_20160607_00000016/budget-debate.
- O'Daffer, A., W. Liu, and C. S. Bloss. 2025. "School-Based Online Surveillance of Youth: Systematic Search and Content Analysis of Surveillance Company Websites." *Journal of Medical Internet Research* 27 (1): e71998. <https://doi.org/10.2196/71998>.
- O'Neill, J. 2011. "The Privatisation of Public Schooling in New Zealand." *Journal of Education Policy* 26 (1): 17–31. <https://doi.org/10.1080/02680939.2010.493227>.
- Pangrazio, L., and J. Sefton-Green. 2021. "Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?" *Journal of New Approaches in Educational Research* 10 (1): 15–27. <https://doi.org/10.7821/naer.2021.1.616>.
- Pleasants, J., X. Gui, D. G. Krutka, C. Logan, and M. K. Heath. 2024. "Coming to Critical Technology Consciousness: A Phenomenological Study of Educators." *Learning, Media and Technology* 1–14. <https://doi.org/10.1080/17439884.2024.2438925>.
- Powell, D.. 2014. "Thinkpiece: Outsourcing: The Hidden Privatisation of Education in New Zealand." *Teachers and Curriculum* 14: 29–32. <https://doi.org/10.15663/tandc.v14i1.91>.
- Privacy Foundation NZ. 2022. *OIA Request to the Ministry of Education Concerning Online Learning – Privacy Foundation NZ Inc, 2 May*. Accessed January 12, 2025. <https://privacyfoundation.nz/oia-request-to-the-ministry-of-education-concerning-online-learning/>.
- Ribble, M.. 2015. *Digital Citizenship in Schools: Nine Elements All Students Should Know*. 3rd ed.. Eugene, OR: International Society for Technology in Education.
- Ribble, M., and G. Bailey. 2007. *Digital Citizenship in Schools*. Eugene, OR: International Society for Technology in Education.
- Rönnerberg, L., M. Benerdal, S. Carlbaum, and A.-S. Holm. 2020. "The Flow of Public Funding to Private Actors in Education: The Swedish Case." In *Privatisation and Commercialisation in Public Education: How the Public Nature of Schooling is Changing*, edited by A. Hogan and Greg Thompson, 134–151. London: Routledge. <https://doi.org/10.4324/9780429330025>.
- Russell, E. 2021. "Really Violent and Terrifying': Teens at Top School Sent Murder and Rape Threats on Snapchat." *NZ Herald*. <https://www.nzherald.co.nz/nz/snapchat-horror-murder-and-rape-threats-sent-to-albany-senior-high-school-students/GEUIOVGEFKCDTLSSCSEUFSVLQY/>.
- Sellar, S., and A. Hogan. 2019. *Pearson 2025: Transforming Teaching and Privatising Education Data*. Education International. <https://www.ei-ie.org/en/item/25681:pearson-2025-transforming-teaching-and-privatising-education-data>.
- Selwyn, N. 2015. "The Discursive Construction of Education in the Digital Age." In *Discourse and Digital Practices: Doing Discourse Analysis in the Digital Age*, edited by R. H. Jones, A. Chik, and C. A. Hafner, 226–240. Abingdon: Routledge. <https://doi.org/10.4324/9781315726465-15>.
- Shepherd, T. 2025. "Grand Social Experiment': Australia's Social Media Ban Turns Heads Globally, with Mixed Results." *The Guardian*. <https://www.theguardian.com/australia-news/2025/dec/10/How-the-world-media-covered-australias-under-16s-social-media-ban>.
- Southgate, E., E. Naghizade, A. Corman, and M. Atherton. 2025. "Towards a Governance Roadmap for Educational Technology in Australian Schools." *The Australian Educational Researcher* 52: 4703–4730. <https://doi.org/10.1007/s13384-025-00916-3>.
- Staksrud, E., and S. Livingstone. 2009. "Children and Online Risk: Powerless Victims or Resourceful Participants?" *Information.* *Communication & Society* 12 (3): 364–387. <https://doi.org/10.1080/13691180802635455>.
- Tan, R. 2022. "Social Media Platforms Duty of Care-Regulating Online Hate Speech." *Australasian Parliamentary Review* 37 (2): 161.
- Tapaleao, V. 2018. "New Zealand School Moving to Ban Facebook." *NZ Herald*. <https://www.nzherald.co.nz/nz/school-tells-parents-ban-Your-kids-from-facebook/714MB5CKWCYPL4WX43KDMYQPS4/>.
- Third, A., P. Collin, L. Walsh, and R. Black. 2019. *Young People in Digital Society: Control Shift*. London: Palgrave Macmillan UK. <https://doi.org/10.1057/978-1-137-57369-8>.
- Thrupp, M., J. O'Neill, D. Powell, and P. Butler. 2020. "Private Actors in New Zealand Schooling: The Path to Saturation." *Journal of Educational Administration and History* 52 (4): 385–402. <https://doi.org/10.1080/00220620.2020.1726882>.
- Tomorrow's Schools Independent Taskforce. 2019. *Our Schooling Futures: Stronger together Whiria Ngā Kura Tūtaititini [Final Report]*. Ministry of Education.
- UNESCO. 2023. *Global Education Monitoring Report 2023: Technology in Education: A Tool on Whose Terms?* (1st ed.). GEM Report UNESCO. <https://doi.org/10.54676/UZQV8501>.

- United Nations, Committee on the Rights of the Child, eds. 2021. *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*. UN. <https://digitallibrary.un.org/record/3906061>.
- Verger, A., C. Fontdevila, and A. Zancajo. 2016. *The Privatization of Education: A Political Economy of Global Education Reform*. New York: Teachers College Press.
- Webster, J. 2024. "Updating Digital Citizenship Education for a Postdigital Society." *New Zealand Journal of Educational Studies* 59 (1): 109–124. <https://doi.org/10.1007/s40841-023-00305-3>.
- Webster, J. 2026. "Schools as Enablers and Constrainers: Teachers' Perceptions and Practices of Digital Citizenship Education in New Zealand." *Learning, Media and Technology* 1–15. <https://doi.org/10.1080/17439884.2026.2625785>.
- Westheimer, J., and J. Kahne. 2004. "What Kind of Citizen? The Politics of Educating for Democracy." *American Educational Research Journal* 41 (2): 237–269. <https://doi.org/10.3102/00028312041002237>.
- Williamson, B., and A. Hogan. 2020. *Commercialisation and Privatisation in/of Education in the Context of Covid-19*. Education International.
- Wishart, J. 2004. "Internet Safety in Emerging Educational Contexts." *Computers & Education* 43 (1): 193–204. <https://doi.org/10.1016/j.compedu.2003.12.013>.
- Wright, N., and M. Peters. 2017. "Sell, Sell, Sell or Learn, Learn, Learn? The EdTech Market in New Zealand's Education System – Privatisation by Stealth?" *Open Review of Educational Research* 4 (1): 164–176. <https://doi.org/10.1080/23265507.2017.1365623>.
- Wylie, C. 2012. *Vital Connections: Why We Need More Than Self-Managing Schools*. Wellington: NZCER Press. <https://www.nzcer.org.nz/nzcerpress/vital-connections>
- Žmavc, J., and L. Z. Bezljaj. 2026. "The EU Policy Discourse on EdTech and Constructing the Image of an Excellent Teacher." *Learning, Media and Technology* 51 (1): 103–116. <https://doi.org/10.1080/17439884.2024.2405859>.
- Zuboff, S.. 2020. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (First Trade Paperback Edition)*. New York: Public Affairs.