Received: 30 May 2024 | Accepted: 2 March 2025

DOI: 10.1002/rev3.70056

ORIGINAL ARTICLE

Review of Education BERA

From safeguarding to critical digital citizenship? A systematic review of approaches to online safety education

Marta Estellés | Andrew Doyle

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

Correspondence
Marta Estellés, Te Kura Toi Tangata School of Education, University of Waikato, Hamilton, New Zealand.
Email: marta.estelles@waikato.ac.nz

Funding information
Spencer Foundation; Division of Education, The University of Waikato

Abstract

Over the last two decades, online safety education has emerged as a new field of research focusing on concerns about a myriad of cyber risks. These risks range from online sexual exploitation through to the reproduction of social inequalities. The main assumption underlying this field is that online risks can be mitigated via educational interventions, and significant discrepancies can be observed between the proposed approaches to online safety education. In this article, we develop an analytical model based on prevalent concepts of digital citizenship and narratives of technologies to identify four different approaches to online safety education in the academic literature; that is, safeguarding, equipping, empowering and resisting. Each of these approaches draws on different assumptions on what constitutes as 'online risk' and 'digital education'. Through a systematic literature review, we analyse 75 journal articles and examine the approaches to online safety education that these studies adopt. Our analysis reveals a dominance of approaches that adopt limited concepts of digital citizenship and acritical views of technology.

KEYWORDS

digital citizenship, digital safety, narratives of technology, online safety

Context and implications

- This article provides an analytical framework that transposes concepts of digital citizenship with narratives of technology. This framework is used to identify approaches towards online safety education in the literature.
- The review found a problematic dominance of acritical views of digital citizenship and technology, which overlook the socio-political contexts and implications of online safety education.
- As this framework considers a broader and more politically situated range of online risks (from cyberbullying and digital exclusion through to discriminatory design and the tyranny of algorithms) and educational solutions (i.e., safeguarding, equipping, empowering and resisting), it serves to enrich current debates about 'digital risks' and has the potential to assist policymakers, researchers and educators to make critically informed decisions regarding online safety education.

INTRODUCTION

With the expansion of Digital Technology (DT) over the last few decades, calls for online safety education (OSE) have become widespread, not only in the media and public debate, but also in the scholarship.[1] This literature, often driven by fears of cyber harms and desires for youth protection, has examined a wide range of dimensions related to this topic, from educators and students' experiences (Adorjan & Ricciardelli, 2019b; Chiner et al., 2023) through to skills frameworks (e.g. Walsh et al., 2022), with the aim of informing the teaching practice that will improve the mitigating of identified risks. The so-called best practices in OSE, however, cannot be considered objective or politically neutral. They are underpinned by different ideological worldviews and understandings of the digital world that influence – and are influenced by – what is considered safe/appropriate and dangerous in these online spaces. Probably the most common critique to the dominant discourse on OSE is being related to the distorted portrayals of students as vulnerable or passive victims and the digital world as a space full of dangers (e.g. Black et al., 2022; Third et al., 2019). As this critique has pointed out, these portrayals have often been used to justify what Third et al. (2019) call the 'control paradigm', which requires limiting young people's agency. Some scholars, however, have also noticed that this safeguarding discourse on OSE is becoming less and less popular (see Third et al., 2019; Third & Collin, 2016). Instead, the literature and policies in this regard seem to be embracing more agentic views of citizenship and less fear-driven portrayals of the digital world, which have led to more 'pro-active' pedagogical initiatives.[2] As a result, the term digital citizenship has received increased attention within OSE discourses with a parallel framing of the digital world as a potential learning space (Black et al., 2022; Third et al., 2019). This does not mean, however, that OSE discourses share common understandings of digital citizenship and/or technologies, nor that they propose similar educational solutions. To consider the complexities involved in this debate, the first part of this article develops an analytical model based on prevalent concepts of digital citizenship and narratives of technologies, which allows us to identify four different approaches to online safety education: that is, safeguarding, equipping, empowering and resisting. The second part of the article uses this model to analyse 75 journal articles and examine the approaches to online safety education that these studies adopt.

APPROACHES TO ONLINE SAFETY EDUCATION

In this section, we develop a model that outlines different approaches to OSE based on the interlinked portrayals of digital citizenship and technology. The model transposes concepts of digital citizenship with narratives of technology, shedding light on different approaches to OSE (see Figure 1). In developing this framework, we seek to expound the different perspectives on citizenship and DT represented, explicitly or implicitly, in the OSE literature. As we explain below, the horizontal axis represents concepts of digital citizenship based on the classic distinction by Westheimer and Kahne (2004) between *personally responsible* and *participatory/justice-oriented* citizenship, frequently used in the literature about digital citizenship education (Heath, 2018; Krutka & Carpenter, 2017); while the vertical axis represents narratives of technology based on the distinction between *techno-optimist* and *technoskeptical* used by Krutka et al. (2022). The combination of both axes in turn gives rise to four different approaches to OSE: *safeguarding*, *equipping*, *empowering* and *resisting*. Each of the approaches are ideal types and, as such, they are the 'result of abstraction and generalisation' and they will only ever approximate to the 'complexity of everyday situated experience' (Dahlberg, 2011, p. 856). Yet, they present a framework through which prevailing approaches of OSE may be explored. In the coming sections, we explain each of the axes in detail.

X axis: Concepts of digital citizenship

As the digital world is consolidated as the main battlefield for the exercise of power (Castells, 2011; Panarari, 2022), digital education debates have increasingly turned their interest towards discussions about citizenship. This shift has generated a prolific scholarly production on the significance and components of this new concept termed 'digital citizenship education' (see Choi, 2016; Emejulu & McGregor, 2019; Frau-Meigs et al., 2017; Ribble, 2015). As a result of this shift, several digital education proposals, including those related to online safety, have broadened their scope to not merely teach technical skills, but also wider civic values and dispositions that regulate online behaviour. Drawing inspiration from other concepts (e.g., 21st century skills, citizenship education, media literacy),

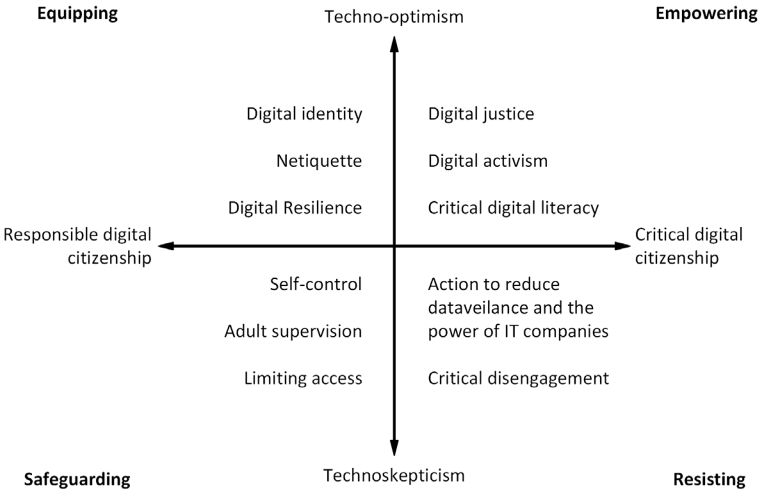

FIGURE 1 Approaches to online safety education.

the literature on digital citizenship education has also been expanded in scope over time (Cortesi et al., 2020).

Despite the growing awareness over the political nature of digital education and the expansion of its components, the increasing use of the term 'digital citizenship' has not always implied an open debate over its ideological underpinnings nor a move towards more critical understanding of the term. Indeed, not openly addressing this debate has often implied a narrow understanding of digital citizenship. For example, as some scholars have pointed out, the implicit definitions of digital citizenship promoted by international societies focused on technology integration, such as the International Society for Technology in Education, are frequently reduced to a 'safe and responsible technology use' (Cortesi et al., 2020; Heath, 2018). A literature review by Heath (2018) concluded that despite the increasing popularity of the term 'digital citizenship', prevalent views are still closely connected to what Westheimer and Kahne (2004) named as *personally responsible* forms of citizenship, which highlight 'appropriate', 'safe' and 'responsible' behaviours online. Heath (2018) also found that *participatory* and *justice-oriented* understandings of citizenship, which emphasise active engagement and the questioning of the status quo (Westheimer & Kahne, 2004), were less common in the literature with some relevant exceptions (Choi, 2016; Gleason & von Gillern, 2018). In the literature on OSE, the debate around the *kind* of digital citizens (Krutka & Carpenter, 2017) has also been largely absent and dominated by thin and paternalistic views of youth citizenship (Black et al., 2022).

The horizontal axis of our proposed model aims to explicitly address the concepts of digital citizenship present within existing approaches to OSE. The axis represents the distinction between personally responsible digital citizenship and participatory/justice-oriented digital citizenship (Krutka & Carpenter, 2017; Westheimer & Kahne, 2004), as it captures the ideological dimension of digital citizenship education obscured in debates around the elements, skills and/or competences. Krutka and Carpenter (2017) describe the first category as a 'responsible, obedient and productive netizen' (p. 52) who is informed and able to 'distinguish between credible and untrustworthy news sources and sites; corroborate information across websites or accounts; contextualize stories; and understand the perspectives, methods and evidence that authors use in multimodal texts' (p. 53). As Heath (2018) points out, this understanding of digital citizenship assumes that 'good character will solve social ills' and, accordingly, examples of educational technology include 'responsible online behaviour and media literacy' (p. 5). The participatory/justice-oriented digital citizen questions political, social and economic structures to fight systemic injustices, organises against oppression and engages in democratic dialogues and civic activities, beyond low-commitment 'slaktivism' (Krutka & Carpenter, 2017, p. 54). This form of citizenship would also align with Emejulu and McGregor's (2019) notion of radical digital citizenship that these scholars describe as:

> …a process by which individuals and groups committed to social justice critically analyse the social, political and economic consequences of digital technologies in everyday life and collectively deliberate and take action to build alternative and emancipatory technologies and technological practices (p. 140)

The distinction between personally responsible and participatory/justice-oriented digital citizenship also encapsulates the components included in other multidimensional models of digital citizenship education. This is the case, for example, of Choi's (2016) review that identified four categories of digital citizenship: ethics, media literacy, engagement and critical resistance. Here, the ethics and media literacy components, which include 'ethical use of technology, digital awareness and digital responsibilities & rights' and 'digital access, technical skills and psychological capability' (Choi, 2016, p. 584), respectively, are indeed essential parts of the personally responsible category. Equally, Choi's (2016) categories of engagement and critical resistance, which include ‘political, economic, cultural engagement and personalized participation’ and ‘critique of the existing power structure and political activism’ (p. 584), respectively, are intrinsically linked to the participatory/justice-oriented digital citizen.

Y axis: Narratives on technology

The idea of technology as a tool of social progress, represented as emancipation or liberalisation, has been dominant in Enlightenment-inspired discourses (Andreotti & Pashby, 2013). This assumption not only operates when the assumed democratic subject is a rational citizen who makes conscious calculations and choices for their best interest, but also when it is understood that citizens are driven by an impetus of social justice (Andreotti & Pashby, 2013; Dahlberg, 2011). For the former, technology provides a venue for rational deliberation and decision-making; for the latter, technology enables the ‘expressions of voice that have been historically marginalised’ (Andreotti & Pashby, 2013, p. 431) and facilitates a platform for self-organised participation beyond the state and capitalist systems (Dahlberg, 2011).

As part of the discourse of modernity, the idea of technology as a vehicle for social progress has also been dominant in educational debates (Krutka et al., 2020) in a narrative that could be termed as *techno-optimist* (Krutka et al., 2022). From this perspective, the affordances of DT are brought to the fore: DT is presented as offering solutions to social problems and therefore need to be embraced. As a result, the core of the educational intervention lies in the mastery of technologies (e.g., learning *how* to best use them and learning *with* them). The optimism inherent to this perspective lies in the ‘production’ of technologically literate citizens that will utilise these technologies for good. In some cases, ‘good’ means for the best interest of the student as an individual-future worker; in others, that ‘good’ refers to leveraging social inequalities. In both cases, however, there is an implicit assumption that technologies are ‘neutral’ instruments, ready to serve the intentions of the user.

These narratives of technological progress and technologies as neutral tools of the *techno-optimist* perspective have received increasing attention in the past few decades. Postman (1992) in their exploration of various technologies throughout history highlighted how the immediate benefits of technologies are often more obvious than the long-term, unintended or collateral consequences. This is perhaps unsurprising as technologies are, by their very nature, designed with a specific purpose in mind. For example, the automobile was developed to facilitate transportation and serves as a very effective solution to travelling short distances in a relatively short amount of time. However, the effect that the automobile would have on employment distributions, shopping patterns and city planning were not immediately apparent (Jackson, 1987). As other technologies have been developed and adopted, similar patterns associated with long-term, unintended or collateral consequences have emerged. This rippling effect is difficult to foresee and more difficult to predict. Within the philosophy of the technology field, *technology criticism* has served as a soundboard through which technological developments and advancements have been critiqued. Recently, an increasing emphasis has been placed on adopting critical views of DT within education rhetoric from a sociological perspective (e.g., Emejulu & McGregor, 2019; Heath, 2018; Krutka et al., 2020; Shelton & Archambault, 2022). As Krutka et al. advocate, there is a need for educational scholars and practitioners to reject the naïve optimist narratives on technology and embrace a *technoskeptical* approach, whereby attention is turned towards ‘the downsides, constraints, or cultural characteristics that technologies extend, amplify, or create’ (2020, p. 111). This approach, as Emejulu and McGregor (2019) would add, also implies an examination of the oppressive relations that make digital technologies possible, such as the exploitation of natural resources and labour in the Global South.

An important point of clarification should be made between the *techno-optimist* and *technoskeptical* perspectives discussed here and the long-established distinction between instrumentalist and determinist views of technology (see Carr, 2011; Feenberg, 2005). To be clear, instrumental and determinist perspectives may be found at both ends of the vertical axis. For example, within the *technoskeptical* narrative of technology, instrumentalist and determinist views of technology may be observed. On the one hand, from an instrumentalist view, individuals may express concerns about the impact of the use of DT on social relationships and mental well-being. The effects of social media and digital communication on interpersonal relationships, and the addictive nature of DT can contribute to feelings of anxiety, distraction and social isolation (Johannessen et al., 2023). The instrumentalist view held here emphasises the consequences of human choices and behaviours. A determinist view of technology on the other hand raises questions about the role of DT in perpetuating 'surveillance capitalism' (Zuboff, 2020) and exacerbating power imbalances in society. The focus here is not on individual 'consumers' of DT, instead attention is turned towards the collection and monetization of personal data by IT companies, leading to concerns about privacy violations, behavioural modification, and the erosion of individual autonomy and democracy (Benjamin, 2020; Zuboff, 2020). Although the narrative of technology in both instances were *technoskeptical*, the concepts of technology, and in turn, solutions to the same risks, differ significantly. As will be further evidenced in the following sections, instrumental and determinist perspectives of technology can also be identified within the techno-optimist approach to DT. In the following sections, we will provide a more detail description of the OSE approaches delineated by this model.

Approach 1: Safeguarding

A safeguarding approach adopts what Third et al. (2019) term the 'control paradigm' approach towards OSE. This approach is driven by fears of online risks and (arguably, paternalistic) child protection desires. These fears and desires are often displayed in detailed recounts of online threats. While there have been several categorisations of online risks in the literature, for example the OECD's typology of risk (2021) and Livingstone and Haddon's (2008) popular classification, the comprehensive framework provided by the UK Department for Education (2023) distinguishes between the 4 Cs of risk management: context, contact, conduct and commerce (see Table 1). In highlighting the risks associated with the digital world, a safeguarding approach uses a security rhetoric that focuses on designing policies and practices aimed at restricting and/or regulating young people's behaviours. There are a variety of different ways in which this may manifest, from adult content control (limiting access to a specific website, etc.), surveillance and regulation of access to DT. Limiting and controlling the exposure of young people to DT is therefore the aims of this approach.

Narrative of technology

The reluctance to engage students with the digital world stems from a technoskeptical view of DT. Rooted in the fear associated with potential risks of DT, technoskepticism can manifest in any number of safety (or security) preventative measures to limit exposure, most often by limiting access to DT. While the affordances of DT may be acknowledged, ultimately the risks outweigh any potential benefits, and engagement with DT is disparaged or regulated. The narrative of technology under this approach has sometimes been described as technophobia (Johannessen et al., 2023).

TABLE 1 Online safety approaches and associated perceptions of problem/risk and solution/safety.

Approach	What is seen as dangerous, risky or unsafe?	What is the solution to the problem of online safety?
Safeguarding	4 Cs risks (Department for Education, 2023). Content: being exposed to illegal, inappropriate or harmful content. Contact: being subjected to harmful online interaction with other users. Conduct: online behaviour that increases the likelihood of, or causes, harm. Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams	Restriction, limited access (online and to digital technologies more generally). Monitor, surveillance and control (so adult intervention can be readily available to stop harm)
Equipping	In addition to the 4 Cs risks, online exclusion: being left outside of the online world, including the inefficient or minimal use of digital technologies, lack of digital access	Learn how to behave responsibly and ethically online (avoiding cyber abuse and promoting netiquette). Develop understanding of digital footprint and learn how to maximise digital identity
Empowering	The reproduction of social inequalities through and within the digital world. e.g., discriminatory design (Benjamin, 2020). Alienation or lack of critical consciousness on systems of oppression. Lack of political participation in online spaces	Critical awareness of social inequalities and the power dynamics reproduced through/within the digital world. Digital activism or mobilisation
Resisting	Loss of privacy (data mining/harvesting/selling, ‘dataveillance’; Clarke, 1988, etc.). The ‘tyranny of algorithms’ (Benasayag, 2021). ‘Filter bubbles’ (Pariser, 2011). The power of IT corporations	Disengagement/resistance from the digital world. Involvement in debates and campaigns to limit power of IT corporations and protect digital rights at national and international scales (Garton Ash, 2016, pp. 92–93)

What kind of digital citizen?

Within a safeguarding approach, the intention is to reduce the possibility of students encountering risks. Digital citizens are therefore understood as those having limited exposure to DT and when they have it, they are expected to adopt cautionary attitudes that protect them from risk. The surveillance/control measures, as Foucault's panopticon, are expected to operate not only to allow adults/supervisors to intervene before harm happens, but also to act as a disciplinary mechanism that would discourage students from engaging in ‘risky’ activities (Adorjan & Ricciardelli, 2019b). These self-regulatory mechanisms are also highly promoted with initiatives such as responsible use agreements. Good digital citizens under this approach are therefore obedient, prudent and self-controlled.

Approach 2: Equipping

The equipping approach to OSE seeks to instil in students' the knowledge and skills to navigate, and benefit from, our increasingly digitised society in a ‘safe’ manner. This approach acknowledges both the potentiality and ubiquity of DT. Thus, the competencies advocated by this approach combine elements to learn from and succeed in the digital world with guidelines around how to act in a responsible manner when online. There is often an acknowledgement of various arenas in which students operate and several discussions have therefore arisen on the components that constitute a comprehensive model from this perspective. Perhaps the most pervasive example of equipping as an approach to OSE are the *9 elements of Digital Citizenship* presented by Ribble and Bailey (2007): digital access, digital commerce, digital communication, digital literacy, digital etiquette, digital law, digital rights and responsibilities, digital health and wellness, and digital security. The preface to Ribble's third edition of the book situates the purpose: 'learn[ing] the fundamentals of acceptable use' (2015, p. 2). Under this approach, the mastering and responsible use of DT in dimensions such as the ones described by Ribble and Bailey (2007) are conceived as a sine qua non condition for individuals not only to keep themselves safe, but also succeed in their lives. For this approach, being online is seen as a necessity and, therefore, being excluded from it (due to safeguarding measures or lack of access) is seen as problematic.

What narrative of technology?

In alignment with the commodification of knowledge, skills or competencies equipped by students, the view of DT is that of something which can be mastered and harnessed for the good of the individual. The slogan of 'technologies are not good nor bad, it depends on the user' is pervasive in this approach and reflects an instrumentalist view of technology. Within this instrumentalist view of technology, DT is used *by* humans, and discussions around digital education centre on providing examples of ways to increase students' technology use and to facilitate safe interactions when engaging with DT. While there is an acknowledgement of the potential harms associated with the use of DT (see Table 1), the benefits, as stated by the advocates of this approach, far outweigh the risks.

What kind of digital citizen?

For this approach, 'good' digital citizens are *active* users of technology for self-improvement (employability, literacy skills, social communication, etc.), yet under the ethical principle of 'not harming others' and a cautionary attitude to prevent abuse from others. Therefore, in this approach (as in safeguarding), the leitmotivs of responsibility and self-control are also present, yet in here the digital citizen is presented as a subject willing to maximise the online experience. Aligned with the instrumentalist view of technology explained above, this approach places learners as digital citizens through the use of DT. As such, the focus of this approach lies in providing students with the skills and values to 'make the most' of the online world.

Approach 3: Empowering

In shifting towards a critical concept of citizenship, this approach is concerned with the reproduction of inequalities in/through the digital world. The focus, therefore, is no longer on the self-realisation of children in the digital world (equipping) or their protection (safeguarding), but on empowering individuals to fight against social injustice. In other words, students are situated in a broader socio-political framework. While it recognises the role of DT in social reproduction, the empowering approach also conceives their potentiality for social action. Advocates are usually inspired by the loose concept of 'critical pedagogy', whereby educators, in an adapted version of the Freirean idea of 'conscientisation', are supposed to help students develop a critical awareness of the digital world through reflection and action. Such digital critical pedagogy involves using DT to both question established, oppressive norms and to engage in consciousness raising dialogues and collective actions (Heath, 2018; Krutka et al., 2019, 2022). What is seen as risky/problematic in this approach, it is not so much a lack of access and/or technical/ethical skills to use DT (i.e., equipping approach), but the lack of: (a) criticality to reflect on how power dynamics are reproduced in society (in and/or through DT), and (b) the skills to organise politically in the digital world.

What narrative of technology?

The empowering approach is clear in acknowledging the downsides of DT, and particularly its functioning in the interest of dominant groups in society. It recognises, for example, forms of discriminatory design, such as ‘engineered inequity, default discrimination, coded exposure and technological benevolence’ (Benjamin, 2020, p. 336), which contribute to the (re)production of social inequality. This approach also condemns the material inequalities and socially exploitative relations involved in the creation of DT (Emejulu & McGregor, 2019). Yet, in keeping with the techno-optimist narrative of technology, DT is viewed as a potential site for political mobilisation and activism to disrupt existing inequalities (Gerbaudo, 2012; Shirky, 2011). In essence, DT is viewed as holding the potential to raise awareness, strengthen community ties and social capital, and facilitate participatory democracy (Heggart & Flowers, 2019), often using an intersectionality lens (e.g., Choi & Cristol, 2021). Therefore, while there is recognition of some of the political constraints imposed by DT, the advocates of this approach still hold, albeit more sophisticated, instrumentalist views of DT, whereby critical citizens and social movements can employ these views in progressive and radical ways. The appropriation of DT by social movements to disseminate information and facilitate networking, organisation and mobilisation (Norris, 2001; Treré, 2019) is the evidence used by this approach to hold the view of DT as a potential tool to pursue social justice ends.

What kind of digital citizen?

The empowering approach is informed by a critical understanding of citizenship, whereby citizens are, in a broad sense, committed to social justice and get organised to fight against systems of oppression (Westheimer & Kahne, 2004). In the digital world, citizens challenge power asymmetries within and through DT (Krutka & Carpenter, 2017), where they are expected to critically examine the corporate influences that affect the uses/misuses of DT and reconsider the ways in which these technologies can be utilised for the sake of social justice and democracy (e.g. Krutka & Carpenter, 2016). An example of this is the development of what Treré (2019) calls ‘algorithms of resistance’, which are seen by activists as a means to harness the power of algorithms to their own advantage. Emejulu and McGregor (2019) call for a ‘collective action for emancipatory technology and technological practice’ that develops ‘independent information platforms, alternative presses, grassroots internet service providers (ISPs), and open source software that support dialogue, organisation and mobilisation outside the confines of corporate media infrastructure’ (p. 142). Another example is formulated by Longford (2005), who advocates for a ‘democratic politics of code’ based on the hacker-inspired open-source software movement through which citizens can design the technical codes that govern their lives. From this perspective therefore, digital citizens should understand how DT regulates and influences people's behaviours and be able to critique existing power structures to envision possibilities for action.

Approach 4: Resisting

In contrast with the previous approaches, the resisting approach is not connected to a particular pedagogical tradition. It is rather a lose educational route map traced by the contributions of critical philosophers, historians, sociologists and journalists (i.e. Benasayag, 2021; Carr, 2011, 2015; Crary, 2022; Han, 2017; Keen, 2015; Zuboff, 2020) that have explored the impact of DT on our societies and strongly question the belief that DT can offer a path towards more democratic societies. From different perspectives, these scholars argue that technologies not only have dangerous consequences that users/consumers cannot escape from (no matter the intention), but also that DT is the product of, and cannot operate outside of, capitalism. They constitute a form of 'instrumentarian power' (Zuboff, 2020) at the service of market imperatives that 'nullify the elemental rights associated with individual autonomy that are essential to the very possibility of a democratic society' (p. 18). For these reasons, these scholars advocate for a resistance to using current DT and a de-virtualisation of social life. What is seen as dangerous from this perspective are the effects of DT on both individuals' abilities and rights (e.g., data mining, commodification of personal information, loss of focus and critical thinking) and democratic projects (e.g., surveillance, consecration of free market ideologies, political polarisation, increasing inequality, concentration of power by IT companies). The sense of agency infused by instrumentalist views of technology and their associated calls to close the digital divide and skills gap are also seen as risky from this perspective. Their argument is that this instrumentalist view of technology is not supported by a sociohistorical analysis of technology (for example, see Carr, 2011). For this approach, the role of the teacher is to help students critically analyse how DT shapes our daily lives and societies (and its dangerous effects for democracy and equality) and consider whether it should be adopted.

What narrative of technology?

This approach is based on a technoskeptical view of technology, which focuses on the downsides, constraints and unintended consequences that DT create or amplify. It is also highly influenced by a determinist view of technology which considers that users cannot merely utilise technology without being, to some extent, used by it. In other words, technologies 'impose' their own modes of social practice, and these modes have profound influences at both micro and macrosocial levels. Advocates of this perspective are concerned with the monetisation of human activity, the architecture of behavioural modification and the increasing power accumulated by IT companies from making users their own product at the expense of their privacy/data (Clarke, 1988; Keen, 2015; Zuboff, 2020).

What kind of digital citizen?

For this approach, critical citizens should perceive the shaping power of DT, examine the social, cultural, economic, political and cognitive effects of their use, and connect these effects with broader social processes, in particular the development of capitalism and neoliberalism.[3] As a result of such analyses, critical citizens are expected to refuse engaging with DT – or, at least, limit its use – due to ethical and political reasons. The 'good' digital citizen here is simply one that resists the seductive and attractive uses of DT, and that decides not to adapt for the safety of democracy, equality and themselves. Also, this citizen is committed to make IT companies accountable for the exploitation of personal information and its effects. In such an endeavour, this citizen gets involved in debates and campaigns to promote legislation at national and international scales that limits the power of these corporations and protects citizens' privacy rights (Garton Ash, 2016).

In the second part of this article, we use the model and approaches to OSE outlined above to analyse their presence in the educational scholarship related to OSE.

Research aim

Using the framework developed above, this study aims to analyse what OSE approaches underlie the educational scholarship focused on OSE.

METHODOLOGY

To address the aim above, we conducted a systematic literature review on digital safety in education. In the following sections we present the methodological approach undertaken, from conducting the literature review to how the identified studies were analysed. The review adhered to the updated Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol (Page et al., 2021). A completed PRISMA protocol checklist has been included in Appendix 1.

Search strategy

Given the breadth of different stakeholders involved with *digital safety* in education, we began by piloting different search criteria. The final inclusion and exclusion criteria are presented in Table 2.

We searched for all records, with no start date and the final search on 15 August 2023. As shown in Table 3, this search yielded a total of 1245 records from the identified databases. The use of Google Scholar® in systematic reviews is somewhat contentious, as the array of sources identified can vary significantly in quality and in quantity. Our search of Google Scholar® returned 17,600 records, for example. We followed the guidance of Haddaway et al. (2015) and included the first 300 records in our initial corpus of literature. It is important to note at this stage that while some of the inclusion and exclusion criteria could have been used as *search limiters* (for example, publication type), our pilot studies identified that databases were not necessarily accurate in their categorisation of publication types. The exclusion and inclusion criteria were instead applied at the title/abstract screening and full-text screening phases, respectively.

TABLE 2 Inclusion and exclusion criteria for this review.

Inclusion criteria	Exclusion criteria
Studies that had *digital safety (education)* as their main focus	Studies where *digital safety (education)* was not the main focus were not considered for inclusion in this study. For example, where digital safety formed part of a broader construct such as digital literacy but was not explicitly defined. In addition, studies that quantified digital safety (for example, as a variable), without presenting any explicit conceptualisation were also excluded
As the focus of this review was on understanding *digital safety education*, we only selected studies on digital safety *for* educational purposes	Studies that focused on digital safety that did not draw implications for education were not considered
Peer-reviewed journal articles	Theses, conference publications, books, book chapters and reports (incl. grey literature)
Full-text article written in English	Full-text articles published in any other languages

TABLE 3 Search syntaxes, databases included, and records returned.

Search syntax	Database	Records returned
'digital safety' OR 'online safety' OR 'cyber safety' OR 'digital risk' OR 'online risk' OR 'cyber risk' AND educ* OR teach* OR learn*	Scopus	*n*=822
	ProQuest Education	*n*=98
	ERIC	*n*=22
	Google Scholar	Returned 17,600 records *n*=300 included

Screening

Once all database searches had been run, the identified records were collated and loaded into Zotero® reference management software where duplicates were identified. Following a manual review of these records, a total of 181 duplicates were removed from the corpus of literature. This yielded a total of 1064 records that were progressed to *publication type* screening. At this stage, our attention turned to records that were not published as journal articles. First, the 1064 records were sorted by *publication type* and all grey literature (theses, conference papers and proceedings, book and book chapters, reports, etc.) were identified based on the source databases categorisation. These records were manually reviewed, and if they were confirmed as grey literature, subsequently removed from the corpus of literature. Alternatively, in the instances where records were miscategorised, they were returned to the main corpus and progressed to title and abstract screening. Concurrently, articles that were categorised as journal articles were reviewed to ensure accuracy. These steps resulted in the identification and subsequent removal of 428 records from the corpus of literature, yielding 636 records that were progressed to title and abstract screening. In a manual review of titles and abstracts, whereby exclusion criteria were used to identify articles, 469 records were identified. The final stage of screening coincided with our preliminary analysis. At this stage, inclusion criteria were used for the first time to ensure that the 167 full-text articles met all the identified criteria for inclusion (Table 2). A total of 75 were selected for inclusion in this study at this final phase of screening (Figure 2).

Data extraction

Following the work of educational scholars developing analytical citizenship frameworks (e.g. Estellés et al., 2023; Johnson & Morris, 2010, 2012), the model developed above was used as a 'heuristic tool' that provided a set of four framing questions to identify relevant information in the articles analysed; (1) How is DT portrayed in this article? (2) What is a 'good' digital citizen according to this article? (3) What is seen as dangerous/risky? And (4) What is the solution proposed for the online safety problem? These questions were used to develop an annotated bibliography template that was used in the first instance to extract data from the individual sources. During this process, we also used Microsoft Excel® to represent the included studies descriptively (see Appendix 2). This process was undertaken with two research assistants. Throughout the process we held multiple meetings whereby those studies difficult to analyse were read concurrently, and discussed until consensus was reached.

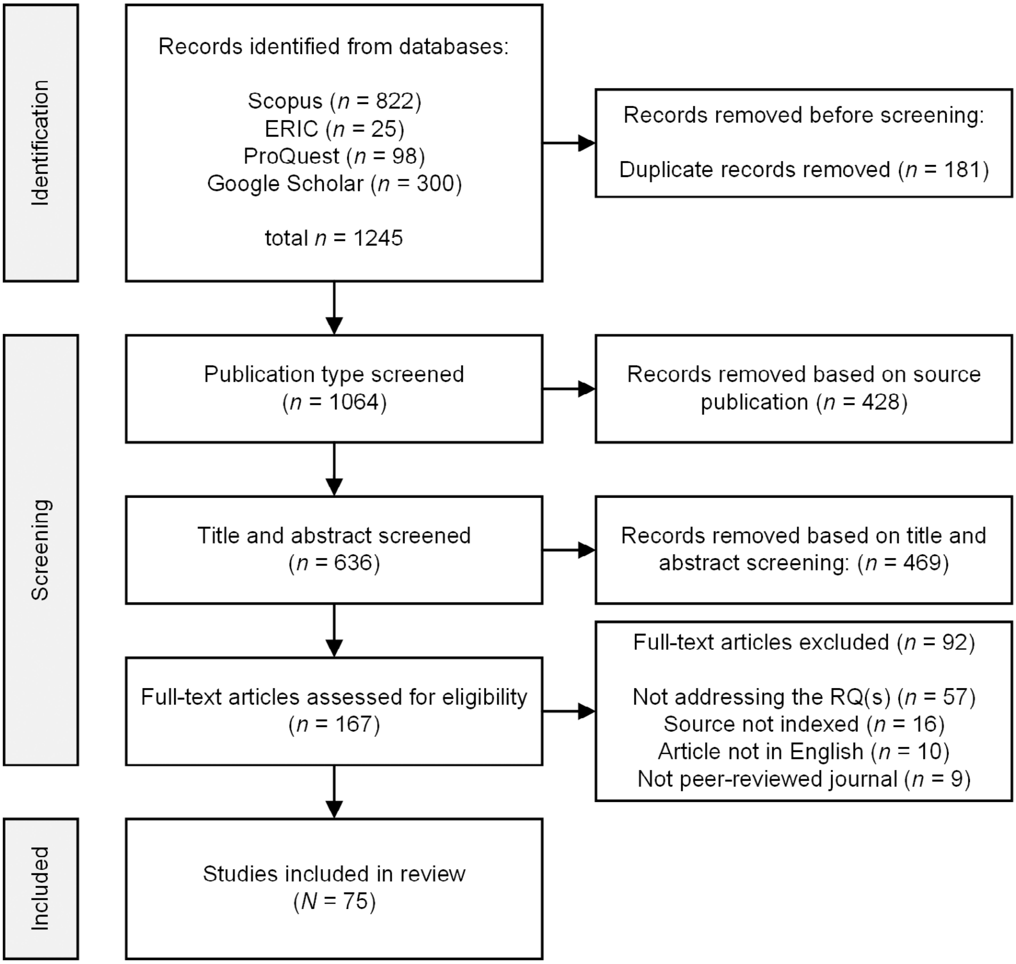
Identification
Records identified from databases:
Scopus (n = 822)
ERIC (n = 25)
ProQuest (n = 98)
Google Scholar (n = 300)
total n = 1245
Records removed before screening:
Duplicate records removed (n = 181)
Screening
Publication type screened (n = 1064)
Records removed based on source publication (n = 428)
Title and abstract screened (n = 636)
Records removed based on title and abstract screening: (n = 469)
Full-text articles assessed for eligibility (n = 167)
Full-text articles excluded (n = 92)
Not addressing the RQ(s) (n = 57)
Source not indexed (n = 16)
Article not in English (n = 10)
Not peer-reviewed journal (n = 9)
Included
Studies included in review (N = 75)

FIGURE 2 Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) diagram of the screening process, showing how records were reviewed through the screening process.

Data analysis

As explained above, the different approaches of OSE are delineated based on the different assumptions of digital citizenship and technology, problem or risk and associated solutions to online safety. In our analysis therefore, we explicitly looked at such assumptions. To identify these assumptions, we focused on 'recurrent concepts, meanings and relationships formed through regularities both within and between descriptions' (Fejes et al., 2018, p. 465). That is, attention was directed at recurring words, phrases deployed, language patterns and statements that reappeared within the analysed texts in relation to the elements included in the questions above. The findings of the analysis are organised around the overarching approaches of the model: safeguarding, equipping, empowering and resisting.

Research limitations and quality assurance

Like all systematic literature reviews, there are some limitations to this review that should be considered. First, this review is limited to English language research published in peer-reviewed journals. Despite the intention of ensuring that only high-quality research is included in the analysis, these decisions will limit the findings as quality work that has been completed in different languages and presented in different publication types (book chapters, theses, conference papers, technical reports, etc.) is not considered for inclusion. This decision was based on the assumption that studies in peer-reviewed journal articles are viewed as being of the highest quality. Although this approach is common within systematic literature reviews (Wilson & Anagnostopoulos, 2021), it should be noted that the development of the findings presented herein through the inclusion of sources from additional sources and language will only serve to further our understanding of OSE.

As the focus of this systematic review was on the OSE *approaches* underlying the OSE literature, sources included a wide variety of forms of scholarship. In other words, we did not impose any specific criteria related to study design or characteristics for quality assurance purposes. As a result of this decision, we included different types of journal articles (for example, empirical and conceptual studies), and ensure our focus on approaches of OSE remained the focus of the research.

FINDINGS

Among the articles included in this review, 12 studies investigated the perceptions or experiences of students, (pre-service) teachers, parents, community stakeholders, etc. on OSE (e.g., Bacak et al., 2022); five explored children's strategies in the digital world (e.g., Hartikainen et al., 2019); seven evaluated the effectiveness of educational interventions (e.g., Schilder et al., 2016); four reviewed the effectiveness of specific educational resources (e.g., Edwards et al., 2020); two examined teachers' practices (e.g., Berger & Wolling, 2019); five specifically investigated children at risk (e.g., Hammond et al., 2023); four reviewed articles on existing research (e.g., Saglam et al., 2023); two developed conceptual frameworks for OSE (e.g., Polizzi & Harrison, 2022); one focused on developing a best practice framework (Walsh et al., 2022); and, finally, one article investigated schools' policies regarding OSE (Siyam & Hussain, 2021).

This overview of articles reviewed is per se quite revealing, as it illustrates an overwhelming emphasis of educational scholarship on school-based issues, rather than on wider socio-political issues. It is important to note that no contextual analyses, such as historical inquiries, policy analyses, analyses of media representations, or investigations on the role of large IT companies, governments, philanthropies and/or private organisations were identified. Perhaps unsurprisingly, the majority of articles point to educators and/or school counsellors as the main solution to online safety, although some isolated articles also mention the responsibility of non-profit companies (Saito et al., 2013) or the IT industry in their solution to online safety (Agha et al., 2023; Kritzinger, 2017a). Even when the role of *key stakeholders* was considered, parents and other professionals, such as clinicians (Moreno et al., 2013), rather than governments or IT companies were identified. By overstating the role of school staff in dealing with online safety problems, these articles, in turn, held teachers responsible for their students' safety:

> Given how central technology is in children's lives, it is essential to recognize and address the host of issues that come along with its usage. School counsellors are in an ideal position to understand online aggression, harassment and

> cyberbullying as students may approach them with these issues (Choudhury & Choudhury, 2023, p. 1095)

This finding is supported by the descriptive analysis of articles analysed using the four approaches to OSE (Figure 1), as articles primarily adopt either safeguarding and/or equipping approaches. We have also identified a few articles sharing elements of equipping and empowering approaches, yet none of the articles reviewed adopted a resisting approach. Also, as Third et al. (2019) noted, there has been a move over time towards more equipping approaches and a consequent abandoning of safeguarding approaches.

Safeguarding

The articles included in this category held assumptions around the risks, narratives of technology, digital citizenship and educational solutions that mostly aligned with the safeguarding approach. Yet, as we explain below, none of these articles can be considered as purely safeguarding, since the majority also include elements of the equipping approach.

What risks?

Most of the articles included in this category were very descriptive of the online risks that children can encounter, using detailed descriptions and/or categorisations. For example, Siyam and Hussain (2021) provide precise definitions of cyberbullying, cybercrime and cybersecurity; Wood and Atkinson's (2015) juxtapose the OECD's typology of risk (2011) that distinguishes between internet technology risks, consumer-related risks and information privacy and security risks with Livingstone and Haddon's (2008) widely adopted classification, the 3 C's of online risks for children: content, contact and conduct.

The language of risk is also more exacerbated with 'vulnerable' populations. See, for example, Caton and Landman's (2022) study on internet safety, online radicalisation and young people with learning disabilities, which include an elaborated section describing risks, such as 'cyberbullying, financial and sexual exploitation and unwanted messages', 'financial and sexual exploitation as well as grooming', 'types of cybercrime', 'grooming for terrorism', etc., and a warning note on the special vulnerability of this group: 'people with learning disabilities who lack understanding of risks engaged in more risk-taking behaviour' (Caton & Landman, 2022, p. 89). Additionally, numerous articles held explicit rationales aligning with equipping approaches; however their portrayal of lack of adult surveillance/control as risky signalled the existence of safeguarding assumptions (Masters & Barr, 2009; Schilder et al., 2016). Masters and Barr's (2009) study on the effectiveness of SuperClubsPLUS (a social networking site for children) provides an illustrative example of this. As explained, this site is a safe environment because 'teachers and mediators can see everything that their students write or create' and 'sophisticated content-checking tools are used by the mediators to monitor all communications, protecting children from bullying or abuse' (Masters & Barr, 2009, p. 297).

What narrative of digital technology?

While the explicit definitions of DT provided by these articles often combined 'positive' and 'negative' elements derived from its use, their emphasis on the risks highlighted above suggests a more technoskeptical view of technology. See, for example, the following rationale articulated by Kritzinger:

> ICT has enormous benefits provided that it is used correctly […] If technology is used incorrectly, it can lead several cyber-related risks and threats which include access to inappropriate material (pornography), personal information being compromised (identity theft), and emotion-related threats (cyber-bullying) (2017a, pp. 16–17).

In addition, as can be seen in the sections below, these articles advocate for a restricted use of DT by children, which also signals their scepticism towards them. Either way, and as can be seen in the quote above, instrumentalist views of technology are prevalent within this approach.

What kind of digital citizens?

Most of the articles adopting safeguarding approaches do not provide explicit definitions of digital citizenship. It is however implied that children are ‘good digital citizens’ when they use DT cautiously, being able to recognise and keep themselves safe from content, contact and conduct risks (e.g., McDonald-Brown et al., 2016) and accept the control/monitoring of adults (e.g., Hanewald, 2008). In some articles, this combination of self-regulation skills and adult supervision is expressed in the listing of ‘cyber-safety rules’ that students need to agree on to become ‘good digital citizens’, which include ‘avoid[ing] opening emails, files or web pages from people I don't know or trust’, ‘always check[ing] with an adult before downloading’, ‘never respond[ing] to strangers online’, ‘tell[ing] an adult if something or someone online makes me feel uncomfortable, scared or confused’ or ‘block[ing] unwanted communication’ (Kritzinger, 2016, p. 12).

What educational solutions?

The educational solutions advocated in the articles included within this category combined elements of equipping (the so-called ‘prevention through education’) with safeguarding measures. See, for example, the following diagram (Figure 3) developed by Hanewald (2008) that summarises the main strategies advocated to deal with cyberbullying, which include, among others, the installation of filtering and blocking software, control software to restrict children's access to internet content, and punitive action, ‘such as the loss of internet privileges for perpetrators, detention or even dismissals from school forever or repeat offenders are other measures’ (p. 13). While Hanewald (2008) is explicit in the advocacy of safeguarding measures, the majority of the articles included in this category combined elements of both equipping and safeguarding approaches and advocated for safeguarding strategies under euphemistic terms, such as ‘management strategies’ (Chiner et al., 2021) or ‘electronic precautions’ (McDonald-Brown et al., 2016).

The use of psychology-informed conceptual frameworks (see, for example, theories of adolescent development in McCarty et al. (2011) and ‘psy’ terminology (intervention, therapy, preventive factors, etc.)) is often use in the advocacy of safeguarding strategies. As explained by Mishna et al. (2009), their literature review analysed prevention and intervention programmes that included: ‘technological and software initiatives […] to block or filter access to inappropriate online content’; ‘Online and offline cyber abuse preventive interventions for parents to protect children from cyber abuse’; and ‘Therapeutic interventions for children and youth who have experienced cyber abuse’ (Mishna et al., 2009, p. 14).

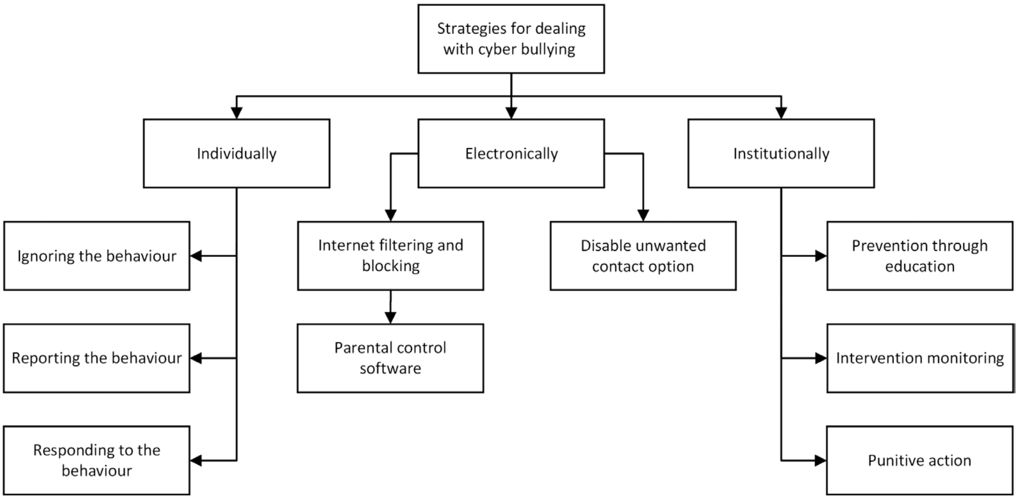
Strategies for dealing with cyber bullying
Individually
Electronically
Institutionally
Ignoring the behaviour
Reporting the behaviour
Responding to the behaviour
Internet filtering and blocking
Parental control software
Disable unwanted contact option
Prevention through education
Intervention monitoring
Punitive action

FIGURE 3 Strategies for dealing with cyberbullying, adapted from Hanewald (2008).

Equipping

Several articles included in this category are based on a critique to safeguarding approaches as legitimate models of OSE. The rationale provided by the equipping approach was inspiring for several articles. The most common argument to disregard safeguarding approaches referred to the 'inefficiency' of their strategies (Bacak et al., 2022; Boulton et al., 2016; Hope, 2010). An example of this argument can be seen below:

> … attempts to attenuate risks by means of parental controls, filters and the like have been shown to be far from effective, and many young people have negative views of parental mediation and often try to avoid it (Boulton et al., 2016, p. 609)

What risks?

The articles included in this category – while recognising the risks central to the safeguarding approach (i.e. 4 C's online risks) – paid more attention to concerns about the lack of knowledge/skills to deal with such dangers. As explained by Ey and Cupit:

> Just under half of the children indicated they had not been taught internet safety. Internet risks for children can be reduced through education in their recognition of potential dangers, recall and management strategies, indicating a need for schools to incorporate internet safety into curricula (Ey & Cupit, 2011, p. 53)

As per the warning given in some articles (Cranmer, 2013; Hammond et al., 2023), the lack of these skills leads to the so-called 'digital exclusion', which is seen as a major risk. As explained by Cranmer (2013), 'some of the young people clearly lacked the basic functional skills needed to use a computer with the internet, therefore placing themselves at risk of digital exclusion' (p. 82). This exclusion is often related to the labour market, as reasoned by Buchanan et al. (2017): 'University admissions and employers are increasingly using digital footprints as a means of verifying identity and perceived suitability of candidates for positions […] A lack of digital footprint can be as damaging as one badly managed' (p. 276).

What narrative of digital technology?

Articles included in this category claim to hold more 'balanced' views of DT than their safeguarding counterparts, by considering the learning opportunities that it offers. A clear example of this narrative is represented by Edwards et al. (2016):

> Cyber-safety awareness is a topic of education that attracts attention as a critical contemporary learning need for all children (Giant 2013). The literature is diverse, and ranges from moral panic regarding children's exposure to unsavoury aspects of the internet, to more measured responses and arguments regarding the pros and cons of children's internet use (p. 326).

What kind of digital citizens?

Unlike the safeguarding literature, these articles provided explicit references to digital citizenship. As explained by Nansen et al., 'Digital citizenship situates online safety within a broader understanding of digital practice by promoting etiquette, literacy and security in an effort to empower children, young people and their families with capacities to participate safely online' (2012, p. 239). For many, in alignment with Ribble's limited definition of digital citizenship (Örtegren, 2023), a good *netizen* behaves in an agentic, responsible and ethical manner (Hipsky & Younes, 2015). Others focus on a single dimension, emphasising, for example, the moral/ethical component of digital citizenship (Polizzi & Harrison, 2022; Pusey & Sadera, 2011). From more agentic perspectives, the concepts of digital resilience and digital identity are embraced (e.g., Buchanan et al., 2017; Choudhury & Choudhury, 2023). The assumption behind these perspectives is that the embracement of DT is inevitable and digital citizens therefore need to be prepared to navigate the risks and maximise their digital identities. Underneath these perspectives, there is also an understanding that citizens need to be prepared to be competitive in the digital world. As explained by Buchanan et al., 'a positive digital footprint can be understood as 'personal brand' that allows others to see your interests, achievements and skills. With the increased reliance on technology, a digital footprint allows for a quick 'google' identity and competency verification' (Buchanan et al., 2017, p. 285).

What educational solutions?

The educational solutions proposed by these articles lie in the *effective* development of knowledge and skills that children need to succeed in the digital world and avoid its risks. Accordingly, some articles focus on the perceived 'best strategies' to do so. Examples of these strategies include cooperative cross-age teaching interventions (Boulton et al., 2016), play-based learning (Edwards, Nolan, et al., 2018), educational materials about social media networking sites (Van der hoven et al., 2016), interactive learning environments (Nicolaidou & Venizelou, 2020), participatory design approaches with children (Buchanan et al., 2017; Edwards et al., 2020), involving industry partners (Edwards et al., 2020) and the use of mobile apps such as MediaKids (Poblet et al., 2017). Other articles provide detailed explanations of the skills on which teachers should focus on, such as digital resilience (Hammond et al., 2023), cyberethics (Pusey & Sadera, 2011), cyber wisdom (Polizzi & Harrison, 2022), cyber-flourishing (Harrison, 2022), self-regulation (Cummings & Cleghorn, 2022), and digital footprint curation (Buchanan et al., 2017).

Empowering

There were only two articles identified as adopting an empowering approach (Black et al., 2022; Chatlani et al., 2023), and, as happened with the safeguarding approach, they were not considered as exclusively empowering, since they shared elements with equipping approach.[4]

What risks?

For Chatlani et al. (2023), what is perceived as risky is the exclusion of particular groups in society from technological design since it contributes to reproduce social inequalities. This risk can be seen in their advocacy of 'justice-centred design':

> Justice-centered design (JCD), within the context of computing, seeks to combat deep societal inequities (e.g., oppression of minorities, labor exploitation and imbalance power dynamics) that have historically been perpetuated through the design of technologies…. In this sense, JCD in the domain of adolescent online safety focuses on addressing the systemic injustices that result from deprioritizing the perspectives and needs of teens in online safety solutions (p. 2)

Similarly, Black et al. (2022) consider as dangerous the denial of full online access and participation for young people. In this approach, they find it problematic that digital technologies have become 'unequal sites for [young people's] political socialisation and practice' rather than 'a liberating and participatory force" (p. 526).

What narrative of digital technology?

For these articles, DT is perceived as the result of power dynamics, yet it also offers a space in which traditionally marginalised groups 'can have a voice about national or global issues' (Black et al., 2022, p. 526) and contribute to their emancipation. Therefore, they hold techno-optimistic (and instrumentalist) views of DT. As explained by Black et al. (2022), acts of digital citizenship 'enable young people first to 'critically analyse the social, political, economic and environmental consequences of technologies in everyday life' and then to 'collectively deliberate and take action to build alternative and emancipatory technologies and technological practices" (p. 526).

What kind of digital citizens?

While not explicitly addressing the question of what digital citizenship means, Chatlani et al. (2023) implicitly understand it from agentic perspectives, in which the good digital citizen is able to participate in the digital world without being subjugated to 'authoritarian control'. From more elaborated definitions, Black et al. (2022) embrace 'an understanding of digital citizenship that encapsulates "young people's rights, responsibilities, conditions and opportunities regarding political and civic participation, cultural identity, solidarity, recognition [and] belonging"' (p. 526).

What educational solutions?

Chatlani et al. (2023) advocate for the use of 'a restorative justice approach, working to combat the historic inequalities that teens have faced in trying to manage their own online safety' (p. 1), which consists of engaging youth in the design of online safety tools. Yet, no further detail is provided, which makes it difficult to gauge the criticality of such tools. Black et al. (2022) also support for a co-development of curricula for OSE with young people, yet they take a step further by highlighting the importance of drawing on young people's digital lived experiences to engage them 'in a critical analysis of their feelings and experiences of membership and identity through the digital' (p. 534).

DISCUSSION

The findings of this review highlight a dominance of approaches towards equipping and safeguarding approaches to OSE. While the equipping approach provides the most inspiring narrative for the literature analysed, the widespread combination of skill development techniques with safeguarding measures suggests that the 'control paradigm' (Third et al., 2019) is still pervasive in OSE debates. Also, this study has found a predominant focus of the literature on pedagogical approaches and school-based issues related to OSE, rather than on policy and/or IT industry. As we explain below, these findings outline two significant and interrelated implications that warrant discussion; that is, the individualisation of social risk and acritical views of technology.

Individualisation of social risk

The dominance of equipping, and to a lesser extent, safeguarding approaches towards OSE identified in this study mirror a broader trend in education of embracing personally responsible concepts of digital citizenship (Heath, 2018), which are highly depoliticised (Emejulu & McGregor, 2019). These views portray the digital citizen as an ethical user of technology who uses technology as part of their participation in 21st century society (Boulton et al., 2016; Cranmer, 2013). Such views are largely influenced by narratives of 'inevitability' (Snyder, 2017) regarding the embracement of DT and the capitalist machinery that sustains them. These views are not only problematic because they ignore the disproportional impact of online risks on particular social groups (e.g., Benjamin, 2020) and the collective struggles that take place online (Castells, 2011), but also because, for them, the individual becomes the only *locus* of potential change, leaving unquestioned the social, cultural, economic and political structures in which digital citizens act and behave. When focusing on the individual, this literature attributes the responsibility of guaranteeing online safety, initially, to teachers and, eventually, to students as 'grown' digital citizens who know how to keep themselves safe. In other words, this literature portrays (good) digital citizens as responsible for their own life choices and risks in the online world. With this individualisation of social risk (Bauman, 2001), attention is focused away from the sources of risks, and from the responsibilities of governments and large IT corporations. Thus, this literature contributes to outsourcing responsibility from governments to protect the rights of citizens online (e.g., privacy rights, principle of non-discrimination) and from IT companies to make sure that the products they provide respect such rights. Despite recent media debates and judicial cases demanding further responsibility from IT companies (Root & Ashford, 2024), educational scholarship largely ignores their role in the provision of an online safe environment. Instead, this literature contributes to the (re)production of neo-liberal citizen subjectivities that have well-internalised their responsibilities in the digital environment and do not question the socio-political, economic and cultural arrangements that maintain it.

In addition to a focus on the individual obfuscating of the role of governments and IT companies, the 'obsession' of the literature with *what happens* or *should happen* in educational contexts prevents researchers from identifying broader developments and trends involved in the provision of OSE. We are referring, for example, to the increasing privatisation of OSE. There is an expansive array of non-profit and for-profit organisations supplying online safety services for 'saturated' schools and transmitting their own views of digital citizenship and technologies (Örtegren, 2023). This phenomenon, however, is largely going unnoticed. This oversight, we argue, is not disconnected from that view of digital citizenship 'stripped of their politics and political implications' (Emejulu & McGregor, 2019, p. 133). When the focus is on individual behaviour modification, the political struggle over what digital citizenship entails is simply overlooked.

The dominance of personally responsible digital citizenship concepts in the literature that contribute to the individualisation of social risk is also closely connected, as Heath (2018) has highlighted, to instrumentalist, acritical views of technology.

Acritical views of technology

Despite many of the articles reviewed highlighting that technology is not value-neutral, and an acknowledgement of both the positives and negatives of technology adoption or use, considerations rarely develop beyond this recognition. A tokenistic acknowledgement of technology as a double-edged sword, without an in-depth consideration of the implications of technology adoption or their political nature, reflects what could be considered an acritical view of technology (Feenberg, 1999, 2006). An example of such a view can be seen in Cummings and Cleghorn's (2022) introduction to the internet as a medium of transmission, in which the authors emphasise how the internet 'makes no distinction between good and bad, and therefore adolescents are required to exercise judgment as they can be subjected to harmful influences and content that may be deemed socially unacceptable' (p. 566). This view was commonly found in the literature reviewed, particularly after acknowledging that research has 'highlighted both the positive and negative effects of digital use on adolescents' development' (Choudhury & Choudhury, 2023). While this approach may be presented as a realistic navigation of contemporary society, in that the ubiquity of DT results in the need to develop appropriate knowledge, skills and competencies, the unquestioned acceptance of DT in tandem with an instrumentalist concept of technology presents a naïve view of the relationship that technology has on society and individuals. This view of DT overlooks its role in the exercise of power, the spread of dominant worldviews, the reproduction of economic structures, and the reinforcement of social inequalities (Benjamin, 2020; Castells, 2011; Zuboff, 2020). In neglecting to interrogate the implicit values and material conditions embedded in digital technology design and development and the impacts of its use, the causes of the challenges posed by DT remained unquestioned. As noted by Emejulu and McGregor (2019), 'constructing technology as innocent or neutral misunderstands the social relations of technology and its very real material consequences in our social world' (p. 133). In this article, we encourage future OSE research to challenge acritical views of technology, whether this manifests as Krutka et al.'s (2020) *technoskepticism* or aligns with the field of technology criticism more generally (Carr, 2011; Feenberg, 2005; Han, 2017; Postman, 1992). We understand that socially and politically informed critiques of digital technology set the foundations for critical forms of digital citizenship education. Indeed, critical educational scholars in this field are increasingly advocating for teaching *about*, rather than *with*, DT to help students rethink their relationship with technology and explore how DT is embedded in the processes of inequality reproduction (e.g., Emejulu & McGregor, 2019; Krutka et al., 2020, 2022). Some of these scholars are also using historical examples of collective movements against technologies as an inspiration to develop pedagogies of resistance (e.g., Logan, 2024). Arguably too, socially and politically informed views of technology allow for educational studies on how DT is affecting critical pedagogies (e.g., Shelton et al., 2022; Shelton & Archambault, 2022). We would like to encourage researchers to engage with and expand this critical work.

CONCLUSION

The framework developed in this article, which transposes views of digital citizenship with narratives of technology, provides an analytical tool to identify approaches towards OSE. In the literature reviewed, scholars mostly rely on safeguarding and equipping approaches towards OSE. These approaches, however, overlook broader socio-political contexts in which calls for OSE take place (a neoliberal context of increasing individualisation of social risk) and the hidden dynamics that happen in the background (e.g., acceptance of lack of privacy rights, lack of accountability from IT corporations, surveillance capitalism, forms of inequality reproduced online). As this framework considers a broader and more politically situated range of online risks and educational solutions, our hope is that it will assist policymakers, researchers and educators to make critically informed decisions regarding OSE.

AUTHOR CONTRIBUTIONS

Marta Estellés: Conceptualization; funding acquisition; writing – original draft; investigation; methodology; writing – review and editing; formal analysis. **Andrew Doyle:** Conceptualization; funding acquisition; writing – original draft; investigation; methodology; writing – review and editing; formal analysis; data curation.

ACKNOWLEDGEMENTS

We would like to express our gratitude to Gurdeep Singh Ghotra for their contributions to preliminary data analysis of this research. We would also like to thank Dr. Florence Lyons for their data analysis and the presentation of findings for this study. Open access publishing facilitated by The University of Waikato, as part of the Wiley - The University of Waikato agreement via the Council of Australian University Librarians.

FUNDING INFORMATION

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

CONFLICT OF INTEREST STATEMENT

On behalf of all authors, the corresponding author states that there is no conflict of interest to report.

ETHICS STATEMENT

As this research only involved the analysis of published materials, ethical approval was not required.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Marta Estellés https://orcid.org/0000-0001-6162-3875
Andrew Doyle https://orcid.org/0000-0003-1993-683X

Endnotes

[1] The recent proliferation of literature reviews related to this topic is an obvious sign of such interest. See, for example, reviews on cybersecurity (Quayyum et al., 2021; Saglam et al., 2023), best practice framework (Walsh et al., 2022), cyberbullying (Brochado et al., 2017; Gaffney et al., 2019; Polanin et al., 2022), sexting (Krieger, 2017), online child sexual abuse (Patterson et al., 2022), youth pornography use (Raine et al., 2020) and sexual solicitation (Wurtele & Kenny, 2016), among others.

[2] See, for example, this change in the policies of the European Union that converted the Safer Internet Programme into the Better Internet for Kids Programme (European Commission, 2022).

[3] Here we use the term 'neoliberalism' to describe both a theory of political-economic practices that posits human well-being can be best improved by promoting individual entrepreneurial freedoms and skills within a strong institutional framework characterised by secure private property rights and free markets (Harvey, 2005, p. 2) and 'a technology of governing "free subjects"' (Ong, 2007, p. 4) that necessitates free and self-managing individuals across various aspects of daily life with expectations of self-responsibility.

[4] It is noteworthy that some articles held elements of empowering, yet they were not included in this category because of their clear connection with the preparation for the labour market, which does not align with the kind of risks and digital citizens underlying this model. This is the case, for example, of Buchanan et al. (2019) with their references to digital exclusion.

REFERENCES

Adorjan, M., & Ricciardelli, R. (2019a). Student perspectives towards school responses to cyber-risk and safety: The presumption of the prudent digital citizen. *Learning, Media and Technology*, *44*(4), 430–442. https://doi.org/10.1080/17439884.2019.1583671

Adorjan, M., & Ricciardelli, R. (2019b). 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

Agha, Z., Badillo-Urquiola, K., & Wisniewski, P. J. (2023). 'Strike at the Root': Co-designing real-time social media interventions for adolescent online risk prevention. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW1), 1–32. https://doi.org/10.1145/3579625

Agosto, D. E., & Abbas, J. (2017). "Don't be dumb—That's the rule I try to live by": A closer look at older teens' online privacy and safety attitudes. *New Media & Society*, *19*(3), 347–365. https://doi.org/10.1177/1461444815606121

Andreotti, V. O., & Pashby, K. (2013). Digital democracy and global citizenship education: Mutually compatible or mutually complicit? *The Educational Forum*, *77*(4), 422–437. https://doi.org/10.1080/00131725.2013.822043

Andrews, J. C., Walker, K. L., & Kees, J. (2020). Children and online privacy protection: Empowerment from cognitive defense strategies. *Journal of Public Policy & Marketing*, *39*(2), 205–219. https://doi.org/10.1177/0743915619883638

Bacak, J., Martin, F., Ahlgrim-Delzell, L., Polly, D., & Wang, W. (2022). Elementary educator perceptions of student digital safety based on technology use in the classroom. *Computers in the Schools*, *39*(2), 186–202. https://doi.org/10.1080/07380569.2022.2071233

Badillo-Urquiola, K., Chouhan, C., Chancellor, S., De Choudhary, M., & Wisniewski, P. (2020). Beyond parental control: Designing adolescent online safety apps using value sensitive design. *Journal of Adolescent Research*, *35*(1), 147–175. https://doi.org/10.1177/0743558419884692

Bauman, Z. (2001). *The individualized society*. Polity Press.

Benasayag, M. (2021). *The tyranny of algorithms: Freedom, democracy, and the challenge of AI*. Europa Editions.

Benjamin, R. (2020). *Race after technology*. Polity.

Berger, P., & Wolling, J. (2019). They need more than technology-equipped schools: Teachers' practice of fostering students' digital protective skills. *Media and Communication*, *7*(2), 137–147. https://doi.org/10.17645/mac.v7i2.1902

Black, R., Walsh, L., Waite, C., Collin, P., Third, A., & Idriss, S. (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

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology*, *34*(10), 1022–1035. https://doi.org/10.1080/0144929X.2015.1028448

Boulton, M. J., Boulton, L., Camerone, E., Down, J., Hughes, J., Kirkbride, C., Kirkham, R., Macaulay, P., & Sanders, J. (2016). Enhancing primary school Children's knowledge of online safety and risks with the CATZ cooperative cross-age teaching intervention: Results from a pilot study. *Cyberpsychology, Behavior, and Social Networking*, *19*(10), 609–614. https://doi.org/10.1089/cyber.2016.0046

Brochado, S., Soares, S., & Fraga, S. (2017). A scoping review on studies of cyberbullying prevalence among adolescents. *Trauma, Violence & Abuse*, *18*(5), 523–531. https://doi.org/10.1177/1524838016641668

Buchanan, R., Southgate, E., & Smith, S. P. (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., Southgate, E., Smith, S. P., Murray, T., & Noble, B. (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

Carr, N. G. (2011). *The shallows: What the internet is doing to our brains*. W.W. Norton.

Carr, N. G. (2015). *The glass cage: How our computers are changing us*. Norton & Company.

Castells, M. (2011). *The rise of the network society* (2nd ed., with a new preface, [reprint]). Wiley-Blackwell.

Caton, S., & Landman, R. (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

Chatlani, N., Davis, A., Badillo-Urquiola, K., Bonsignore, E., & Wisniewski, P. (2023). Teen as research-apprentice: A restorative justice approach for centering adolescents as the authority of their own online safety. *International Journal of Child-Computer Interaction*, *35*, 100549. https://doi.org/10.1016/j.ijcci.2022.100549

Chiner, E., Gómez-Puerta, M., & Cardona-Moltó, M. C. (2023). Digital inclusion in Spanish mainstream and special schools: Teachers' perceptions of internet use by students with intellectual disabilities. *British Journal of Learning Disabilities*, *51*(2), 195–204. https://doi.org/10.1111/bld.12503

Chiner, E., Gómez-Puerta, M., & Mengual-Andrés, S. (2021). Opportunities and hazards of the internet for students with intellectual disabilities: The views of pre-service and in-service teachers. *International Journal of Disability, Development and Education*, *68*(4), 538–553. https://doi.org/10.1080/1034912X.2019.1696950

Choi, M. (2016). A concept analysis of digital citizenship for democratic citizenship education in the internet age. *Theory & Research in Social Education*, *44*(4), 565–607. https://doi.org/10.1080/00933104.2016.1210549

Choi, M., & Cristol, D. (2021). Digital citizenship with intersectionality lens: Towards participatory democracy driven digital citizenship education. *Theory Into Practice*, *60*(4), 361–370. https://doi.org/10.1080/00405841.2021.1987094

Chou, H.-L., & Sun, J. C.-Y. (2017). The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers. *Computers in Education*, *112*, 83–96. https://doi.org/10.1016/j.compedu.2017.05.003

Choudhury, T., & Choudhury, R. (2023). Digital experiences of children and adolescents in India: New challenges for school counsellors. *Psychology in the Schools*, *60*(4), 1094–1106. https://doi.org/10.1002/pits.22821

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512.

Cortesi, S., Hasse, A., Lombana-Bermudez, A., Kim, S., & Gasser, U. (2020). *Youth and digital citizenship+ (plus): Understanding skills for a digital world*. Berkman Klein Center for Internet & Society. https://dash.harvard.edu/handle/1/42638976

Cranmer, S. (2013). Listening to excluded young people's experiences of e-safety and risk. *Learning, Media and Technology*, *38*(1), 72–85. https://doi.org/10.1080/17439884.2012.658405

Crary, J. (2022). *Scorched earth: Beyond the digital age to a post-capitalist world*. Verso.

Cummings, C. A., & Cleghorn, L. L. (2022). Exploring adolescents' vulnerability and resilience to online risks in Trinidad and Tobago. *Journal of Children and Media*, *16*(4), 565–574. https://doi.org/10.1080/17482798.2022.2072921

Dahlberg, L. (2011). Re-constructing digital democracy: An outline of four 'positions'. *New Media & Society*, *13*(6), 855–872.

Department for Education. (2023). *Keeping children safe in education 2023: Statutory guidance for schools and colleges*. Department for Education. https://assets.publishing.service.gov.uk/media/64f0a68ea78c5f000dc6f3b2/Keeping_children_safe_in_education_2023.pdf

El Asam, A., & Katz, A. (2018). Vulnerable young people and their experience of online risks. *Human-Computer Interaction*, *33*(4), 281–304. https://doi.org/10.1080/07370024.2018.1437544

Edwards, S., Mantilla, A., Henderson, M., Nolan, A., Skouteris, H., & Plowman, L. (2018). Teacher practices for building Young Children's concepts of the internet through play-based learning. *Educational Practice and Theory*, *40*(1), 29–50. https://doi.org/10.7459/ept/40.1.03

Edwards, S., Nolan, A., Henderson, M., Grieshaber, S., Highfield, K., Salamon, A., Skouteris, H., & Straker, L. (2020). Rationale, design and methods protocol for participatory design of an online tool to support industry service provision regarding digital technology use 'with, by and for' young children. *International Journal of Environmental Research and Public Health*, *17*(23), 1–12. https://doi.org/10.3390/ijerph17238819

Edwards, S., Nolan, A., Henderson, M., Mantilla, A., Plowman, L., & Skouteris, H. (2018). Young children's everyday concepts of the internet: A platform for cyber-safety education in the early years. *British Journal of Educational Technology*, *49*(1), 45–55. https://doi.org/10.1111/bjet.12529

Edwards, S., Nolan, A., Henderson, M., Skouteris, H., Mantilla, A., Lambert, P., & Bird, J. (2016). Developing a measure to understand young children's internet cognition and cyber-safety awareness: A pilot test. *Early Years*, *36*(3), 322–335. https://doi.org/10.1080/09575146.2016.1193723

Emejulu, A., & McGregor, C. (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

Estellés, M., Oliveira, A., & Castellví, J. (2023). National curricula and citizenship education in populist times. The cases of Brazil and Spain. *Compare: A Journal of Comparative and International Education*, *54*(6), 1–19. https://doi.org/10.1080/03057925.2023.2170167

European Commission. (2022). *Communication from the commission to the European Parliament, the council, the European economic and social committee and the Committee of the Regions: A digital decade for children and youth: The new European strategy for a better internet for kids (BIK+)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212

Ey, L.-A., & Cupit, C. G. (2011). Exploring young children's understanding of risks associated with internet usage and their concepts of management strategies. *Journal of Early Childhood Research*, *9*(1), 53–65. https://doi.org/10.1177/1476718X10367471

Feenberg, A. (1999). *Questioning technology*. Routledge.

Feenberg, A. (2005). Critical theory of technology: An overview. *Tailoring Biotechnologies*, *1*(1), 47–64.

Feenberg, A. (2006). What is philosophy of technology? In J. R. Dakers (Ed.), *Defining technological literacy: Towards an epistemological framework* (pp. 5–16). Palgrave Macmillan. https://doi.org/10.1057/9781403983053_2

Fejes, A., Olson, M., Rahm, L., Dahlstedt, M., & Sandberg, F. (2018). Individualisation in Swedish adult education and the shaping of neo-liberal subjectivities. *Scandinavian Journal of Educational Research*, *62*(3), 461–473. https://doi.org/10.1080/00313831.2016.1258666

Frau-Meigs, D., O'Neill, B., Soriani, A., & Tomé, V. (2017). *Overview and new perspectives*. Council of Europe.

Gaffney, H., Farrington, D. P., Espelage, D. L., & Ttofi, M. M. (2019). Are cyberbullying intervention and prevention programs effective? A systematic and meta-analytical review. *Aggression and Violent Behavior*, *45*, 134–153. https://doi.org/10.1016/j.avb.2018.07.002

Garton Ash, T. (2016). *Free speech: Ten principles for a connected world*. Yale University Press.

Gerbaudo, P. (2012). *Tweets and the streets: Social media and contemporary activism*. Pluto Press.

Gleason, B., & von Gillern, S. (2018). Digital citizenship with social media: Participatory practices of teaching and learning in secondary education. *Journal of Educational Technology & Society*, *21*(1), 200–212.

Haddaway, N. R., Collins, A. M., Coughlin, D., & Kirk, S. (2015). The role of Google scholar in evidence reviews and its applicability to Grey literature searching. *PLoS One*, *10*(9), e0138237. https://doi.org/10.1371/journal.pone.0138237

Hammond, S. P., D'Arcy, J., Minott, M., & Krasniqi, E. (2023). A discursive psychological examination of educators' experiences of children with disabilities accessing the Internet: a role for digital resilience. *Information, Communication & Society*, *27*(1), 161–181. https://doi.org/10.1080/1369118X.2023.2185103

Han, B.-C. (2017). *In the swarm: Digital prospects (E. Butler, Trans.)*. MIT Press.

Hanewald, R. (2008). Confronting the pedagogical challenge of cyber safety. *Australian Journal of Teacher Education*, *33*(3), 1–16. https://doi.org/10.14221/ajte.2008v33n3.1

Harrison, T. (2022). A new educational model for online flourishing: A pragmatic approach to integrating moral theory for cyber-flourishing. *Pastoral Care in Education*, *40*(2), 128–151. https://doi.org/10.1080/02643944.2021.1898665

Hartikainen, H., Iivari, N., & Kinnula, M. (2019). Children's design recommendations for online safety education. *International Journal of Child-Computer Interaction*, *22*, 100146. https://doi.org/10.1016/j.ijcci.2019.100146

Harvey, D. (2005). *A brief history of neoliberalism*. Oxford University Press.

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

Heggart, K., & Flowers, R. (2019). Justice citizens, active citizenship, and critical pedagogy: Reinvigorating citizenship education. *Democracy and Education*, *27*(1), 2.

Hernández-Martín, A., Martín-del-Pozo, M., & Iglesias-Rodríguez, A. (2021). Pre-adolescents' digital competences in the area of safety. Does frequency of social media use mean safer and more knowledgeable digital usage? *Education and Information Technologies*, *26*(1), 1043–1067. https://doi.org/10.1007/s10639-020-10302-4

Hina, S., & Dominic, P. D. D. (2016). Gauging the school-based acceptability of web 2.0 collaborative tools. *International Journal of Business Information Systems*, *21*(3), 321–341. https://doi.org/10.1504/IJBIS.2016.074761

Hipsky, S., & Younes, W. (2015). Beyond concern: K-12 faculty and staff's perspectives on privacy topics and Cybersafety. *International Journal of Information and Communication Technology Education*, *11*(4), 51–66. https://doi.org/10.4018/IJICTE.2015100104

Hope, A. (2010). Seductions of risk and school cyberspace. *Australasian Journal of Educational Technology*, *26*(5), 690–703. https://doi.org/10.14742/ajet.1059

Jackson, K. T. (1987). *Crabgrass frontier: The suburbanization of the United States*. Oxford University Press.

Johannessen, L. E. F., Rasmussen, E. B., & Haldar, M. (2023). Educational purity and technological danger: Understanding scepticism towards the use of telepresence robots in school. *British Journal of Sociology of Education*, *44*(4), 703–719. https://doi.org/10.1080/01425692.2023.2203360

Johnson, L., & Morris, P. (2010). Towards a framework for critical citizenship education. *The Curriculum Journal*, *21*(1), 77–96. https://doi.org/10.1080/09585170903560444

Johnson, L., & Morris, P. (2012). Critical citizenship education in England and France: A comparative analysis. *Comparative Education*, *48*(3), 283–301. https://doi.org/10.1080/03050068.2011.588885

Keen, A. (2015). *The internet is not the answer* (1st ed.). Atlantic Books.

Krieger, M. A. (2017). Unpacking "sexting": A systematic review of nonconsensual sexting in legal, educational, and psychological literatures. *Trauma, Violence & Abuse*, *18*(5), 593–601. https://doi.org/10.1177/1524838016659486

Kritzinger, E. (2016). Short-term initiatives for enhancing cyber-safety within south African schools. *South African Computer Journal*, *28*(1), 1–17. https://doi.org/10.18489/sacj.v28i1.369

Kritzinger, E. (2017a). Cultivating a cyber-safety culture among school learners in South Africa. *Africa Education Review*, *14*(1), 22–41. https://doi.org/10.1080/18146627.2016.1224561

Kritzinger, E. (2017b). Growing a cyber-safety culture amongst school learners in South Africa through gaming. South African. *Computer Journal*, *29*(2), 16–35. https://doi.org/10.18489/sacj.v29i2.471

Kritzinger, E. (2020). Improving cybersafety maturity of south African schools. *Information (Switzerland)*, *11*(10), 471. https://doi.org/10.3390/info11100471

Krutka, D. G., & Carpenter, J. P. (2016). Mediating democracy: Social media as curriculum. In *Teaching for democracy in an age of economic disparity* (pp. 235–354). Routledge.

Krutka, D. G., & Carpenter, J. P. (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., Heath, M. K., & Mason, L. E. (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., Heath, M. K., & Willet, K. B. S. (2019). Foregrounding Technoethics: Toward critical perspectives in technology and teacher education. *Journal of Technology and Teacher Education*, *27*(4), 555–574.

Krutka, D. G., Metzger, S. A., & Seitz, R. Z. (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

Livingstone, S., & Haddon, L. (2008). Risky experiences for children online: Charting European research on children and the internet. *Children and Society*, *22*(4), 314–323. https://doi.org/10.1111/j.1099-0860.2008.00157.x

Logan, C. (2024). Learning about and against generative AI through mapping generative AI's ecologies and developing a luddite praxis. In R. Lindgren, T. I. Asino, E. A. Kyza, C. K. Looi, D. T. Keifert, & E. Suárez (Eds.), *Proceedings of the 18th international conference of the learning sciences – ICLS* (pp. 362–369). International Society of the Learning Sciences. https://doi.org/10.22318/icls2024.259570

Longford, G. (2005). Pedagogies of digital citizenship and the politics of code. *Techné: Research in Philosophy and Technology*, *9*(1), 68–96. https://doi.org/10.5840/techne2005916

Lorenz, B., Kikkas, K., & Laanpere, M. (2012). Comparing children's e-safety strategies with guidelines offered by adults. *Electronic Journal of E-Learning*, *10*(3), 326–338.

Mabitle, K., & Kritzinger, E. (2021). Predicting Schoolteachers' intention and behaviour of promoting cyber-safety awareness. *International journal of information and education technology*, *11*(3), 119–125. https://doi.org/10.18178/ijiet.2021.11.3.1499

Macaulay, P. J. R., Boulton, M. J., Betts, L. R., Boulton, L., Camerone, E., Down, J., Hughes, J., Kirkbride, C., & Kirkham, R. (2020). Subjective versus objective knowledge of online safety/dangers as predictors of children's perceived online safety and attitudes towards e-safety education in the United Kingdom. *Journal of Children and Media*, *14*(3), 376–395. https://doi.org/10.1080/17482798.2019.1697716

Martin, F., Bacak, J., Polly, D., Wang, W., & Ahlgrim-Delzell, L. (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

Martin, N., & Rice, J. (2012). Children's cyber-safety and protection in Australia: An analysis of community stakeholder views. *Crime Prevention and Community Safety*, *14*(3), 165–181. https://doi.org/10.1057/cpcs.2012.4

Masters, J., & Barr, S. (2009). Young children online: E-learning in a social networking context. *Knowledge Management and E-Learning*, *1*(4), 295–304.

McCarty, C., Prawitz, A. D., Derscheid, L. E., & Montgomery, B. (2011). Perceived safety and teen risk taking in online chat sites. *Cyberpsychology, Behavior, and Social Networking*, *14*(3), 169–174. https://doi.org/10.1089/cyber.2010.0050

McDonald-Brown, C., Laxman, K., & Hope, J. (2016). An exploration of the contexts, challenges and competencies of pre-teenage children on the internet. *International Journal of Technology Enhanced Learning*, *8*(1), 1–25. https://doi.org/10.1504/IJTEL.2016.075949

McDonald-Brown, C., Laxman, K., & Hope, J. (2017). Sources of support and mediation online for 9–12-year-old children. *E-Learning and Digital Media*, *14*(1–2), 52–71. https://doi.org/10.1177/2042753017692430

Mishna, F., Cook, C., Saini, M., Wu, M.-J., & MacFadden, R. (2009). Interventions for children, youth, and parents to prevent and reduce cyber abuse. *Campbell Systematic Reviews*, *5*(1), 1–54. https://doi.org/10.4073/csr.2009.2

Moreno, M. A., Egan, K. G., Bare, K., Young, H. N., & Cox, E. D. (2013). Internet safety education for youth: Stakeholder perspectives. *BMC Public Health*, *13*(1), 543. https://doi.org/10.1186/1471-2458-13-543

Nansen, B., Chakraborty, K., Gibbs, L., MacDougall, C., & Vetere, F. (2012). Children and digital wellbeing in Australia: Online regulation, conduct and competence. *Journal of Children and Media*, *6*(2), 237–254. https://doi.org/10.1080/17482798.2011.619548

Nicolaidou, I., & Venizelou, A. (2020). Improving children's E-safety skills through an interactive learning environment: A quasi-experimental study. *Multimodal Technologies and Interaction*, *4*(2), 10. https://doi.org/10.3390/mti4020010

Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the internet worldwide* (1st ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139164887

OCED. (2011). *The protection of children online risks faced by children online and policies to protect them. (179; OECD digital economy papers)*. OECD Publishing. https://doi.org/10.1787/5kgcjf71pl28-en

OECD. (2021). *Children in the digital environment: Revised typology of risks (302)*. OECD Publishing. https://doi.org/10.1787/9b8f222e-en

Ondrušková, D., & Pospíšil, R. (2023). The good practices for implementation of cyber security education for school children. *Contemporary Educational Technology*, *15*(3), ep435. https://doi.org/10.30935/cedtech/13253

Ong, A. (2007). Neoliberalism as a mobile technology. *Transactions of the Institute of British Geographers*, *32*(1), 3–8. https://doi.org/10.1111/j.1475-5661.2007.00234.x

O'Reilly, D., & O'Neill, C. (2008). An analysis of Irish primary school children's internet usage and the associated safety implications. *International Journal of Information and Communication Technology Education*, *4*(3), 40–48. https://doi.org/10.4018/jicte.2008070105

Örtegren, A. (2023). Philosophical underpinnings of digital citizenship through a postdigital lens: Implications for teacher educators' professional digital competence. *Education and Information Technologies*, *29*(4), 4253–4285. https://doi.org/10.1007/s10639-023-11965-5

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Systematic Reviews*, *10*(1), 89. https://doi.org/10.1186/s13643-021-01626-4

Panarari, M. (2022). The transformations of "public sphere" category, and the contemporary debate about digital citizenship. *Journal of E-Learning and Knowledge Society*, *18*(3), 1–7. https://doi.org/10.20368/1971-8829/1135814

Pariser, E. (2011). *The filter bubble: What the internet is hiding from you*. Viking.

Patterson, A., Ryckman, L., & Guerra, C. (2022). A systematic review of the education and awareness interventions to prevent online child sexual abuse. *Journal of Child and Adolescent Trauma*, *15*(3), 857–867. https://doi.org/10.1007/s40653-022-00440-x

Poblet, M., Teodoro, E., González-Conejero, J., Varela, R., & Casanovas, P. (2017). A co-regulatory approach to stay safe online: Reporting inappropriate content with the MediaKids mobile app. *Journal of Family Studies*, *23*(2), 180–197. https://doi.org/10.1080/13229400.2015.1106337

Polanin, J. R., Espelage, D. L., Grotpeter, J. K., Ingram, K., Michaelson, L., Spinney, E., Valido, A., Sheikh, A. E., Torgal, C., & Robinson, L. (2022). A systematic review and meta-analysis of interventions to decrease cyberbullying perpetration and victimization. *Prevention Science*, *23*(3), 439–454. https://doi.org/10.1007/s11121-021-01259-y

Polizzi, G., & Harrison, T. (2022). Wisdom in the digital age: A conceptual and practical framework for understanding and cultivating cyber-wisdom. *Ethics and Information Technology*, *24*(1), 16. https://doi.org/10.1007/s10676-022-09640-3

Postman, N. (1992). *Technopoly: The surrender of culture to technology*. Alfred A. Knopf, Inc.

Purnama, S., Ulfah, M., Machali, I., Wibowo, A., & Narmaditya, B. S. (2021). Does digital literacy influence students' online risk? Evidence from Covid-19. *Heliyon*, *7*(6), e07406. https://doi.org/10.1016/j.heliyon.2021.e07406

Pusey, P., & Sadera, W. A. (2011). Cyberethics, Cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education*, *28*(2), 82–85. https://doi.org/10.1080/21532974.2011.10784684

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Raine, G., Khouja, C., Scott, R., Wright, K., & Sowden, A. J. (2020). Pornography use and sexting amongst children and young people: A systematic overview of reviews. *Systematic Reviews*, *9*(1), 283. https://doi.org/10.1186/s13643-020-01541-0

Ribble, M. (2015). *Digital citizenship in schools: Nine elements all students should know* (3rd ed.). International Society for Technology in Education.

Ribble, M., & Bailey, G. D. (2007). *Digital citizenship in schools* (1st ed.). International Society for Technology in Education.

Root, J., & Ashford, G. (2024). Inside a High-Stakes Fight to Limit Social Media's Hold on Children. *The New York Times*. https://www.nytimes.com/2024/03/29/nyregion/social-media-algorithms-children.html

Saglam, R. B., Miller, V., & Franqueira, V. N. L. (2023). A systematic literature review on cyber security education for children. *IEEE Transactions on Education*, *66*(3), 274–286. https://doi.org/10.1109/TE.2022.3231019

Saito, N., Tanaka, E., & Yatsuzuka, E. (2013). Evolving challenges to the development and assessment of information literacy education for online safety in Japan. *Journal of Cases on Information Technology*, *15*(4), 21–44. https://doi.org/10.4018/jcit.2013100103

Schilder, J. D., Brusselaers, M. B. J., & Bogaerts, S. (2016). The effectiveness of an intervention to promote awareness and reduce online risk behavior in early adolescence. *Journal of Youth and Adolescence*, *45*(2), 286–300. https://doi.org/10.1007/s10964-015-0401-2

Shelton, C., & Archambault, L. (2022). Educators engaging in online educational marketplaces: A vision for teacher education to prepare critical consumers, careful creators, and discerning professionals. *Journal of Technology and Teacher Education*, *30*(2), 155–166.

Shelton, C., Curcio, R., Carpenter, J. P., & Schroeder, S. E. (2022). Instagramming for justice: The potentials and pitfalls of culturally relevant professional learning on Instagram. *TechTrends*, *66*(5), 837–854. https://doi.org/10.1007/s11528-022-00758-1

Shin, W., & Lwin, M. O. (2017). How does “talking about the internet with others” affect teenagers' experience of online risks? The role of active mediation by parents, peers, and school teachers. *New Media & Society*, *19*(7), 1109–1126. https://doi.org/10.1177/1461444815626612

Shirky, C. (2011). The political power of social media: Technology, the public sphere, and political change. *Foreign Affairs*, *90*(1), 28–41.

Siyam, N., & Hussain, M. (2021). Cyber-safety policy elements in the era of online learning: A content analysis of policies in the UAE. *TechTrends*, *65*(4), 535–547. https://doi.org/10.1007/s11528-021-00595-8

Snyder, T. (2017). *On tyranny: Twenty lessons from the twentieth century* (1st ed.). Tim Duggan Books.

Teimouri, M., Benrazavi, S. R., Griffiths, M. D., & Hassan, M. S. (2018). A model of online protection to reduce Children's online risk exposure: Empirical evidence from Asia. *Sexuality and Culture*, *22*(4), 1205–1229. https://doi.org/10.1007/s12119-018-9522-6

Third, A., & Collin, P. (2016). Rethinking (children's and young people's) citizenship through dialogues on digital practice. In A. McCosker, S. Vivienne, & A. Johns (Eds.), *Negotiating digital citizenship: Control, contest and culture* (pp. 41–60). Rowman & Littlefield.

Third, A., Collin, P., Walsh, L., & Black, R. (2019). *Young people in digital society: Control shift*. Palgrave Macmillan UK. https://doi.org/10.1057/978-1-137-57369-8

Tick, A., Cranfield, D. J., Venter, I. M., Renaud, K. V., & Blignaut, R. J. (2021). Comparing three countries' higher education students' cyber related perceptions and behaviours during COVID-19. *Electronics (Switzerland)*, *10*(22), 2865. https://doi.org/10.3390/electronics10222865

Tomczyk, Ł. (2019). What do teachers know about digital safety? *Computers in the Schools*, *36*(3), 167–187. https://doi.org/10.1080/07380569.2019.1642728

Touloupis, T., & Athanasiades, C. (2020). A comparison between primary school principals' and teachers' perceptions of students' online risk behaviours: The role of perceived self-efficacy. *Cambridge Journal of Education*, *50*(4), 1–18. https://doi.org/10.1080/0305764X.2020.1740170

Treré, E. (2019). *Hybrid media activism: Ecologies, imaginaries, algorithms*. Routledge, Taylor & Francis Group.

Tsimtsiou, Z., Drosos, E., Drontsos, A., Haidich, A.-B., Dantsi, F., Sekeri, Z., Dardavesis, T., Nanos, P., & Arvanitidou, M. (2021). Raising awareness on cyber safety: Adolescents' experience of a primary healthcare professional-led, school-based, multi-center intervention. *International Journal of Adolescent Medicine and Health*, *31*(6), 20170072. https://doi.org/10.1515/ijamh-2017-0072

Van der hoven, E., Schellens, T., Van der linde, R., & Valcke, M. (2016). Developing educational materials about risks on social network sites: A design based research approach. *Educational Technology Research and Development*, *64*(3), 459–480. https://doi.org/10.1007/s11423-015-9415-4

Van derhoven, E., Schellens, T., & Valcke, M. (2013). Exploring the usefulness of school education about risks on social network sites: A survey study. *Journal of media literacy Education*, *5*(1), 285–294. https://doi.org/10.23860/jmle-5-1-2

Vila-Counago, E., Regueira, U., & Pernas-Morado, E. (2020). The safety area of digital competence: A mixed method study in Galician primary education students. *Revista Iberoamericana de Tecnologias Del Aprendizaje*, *15*(4), 389–398. https://doi.org/10.1109/RITA.2020.3033218

Walsh, K., Pink, E., Ayling, N., Sondergeld, A., Dallaston, E., Tournas, P., Serry, E., Trotter, S., Spanos, T., & Rogic, N. (2022). Best practice framework for online safety education: Results from a rapid review of the international literature, expert review, and stakeholder consultation. *International Journal of Child-Computer Interaction*, *33*, 100474. https://doi.org/10.1016/j.ijcci.2022.100474

Westheimer, J., & Kahne, J. (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

Wilson, S. M., & Anagnostopoulos, D. (2021). Methodological Guidance Paper: The Craft of Conducting a Qualitative Review. *Review of Educational Research*, *91*(5), 651–670. https://doi.org/10.3102/00346543211012755

Wood, R., & Atkinson, S. (2015). Student teachers' perceptions of online risk. *International Journal of Technologies in Learning*, *23*(1), 1–10. https://doi.org/10.18848/2327-0144/cgp/v23i01/49082

Wurtele, S. K., & Kenny, M. C. (2016). Technology-related sexual solicitation of adolescents: A review of prevention efforts. *Child Abuse Review*, *25*(5), 332–344. https://doi.org/10.1002/car.2445

Zuboff, S. (2020). *The age of surveillance capitalism: The fight for a human future at the new frontier of power (First trade paperback edition)*. PublicAffairs.

How to cite this article: Estellés, M., & Doyle, A. (2025). From safeguarding to critical digital citizenship? A systematic review of approaches to online safety education. *Review of Education*, *13*, e70056. https://doi.org/10.1002/rev3.70056

APPENDIX 1

PRISMA checklist (Page et al., 2021)

Section and topic	Item #	Checklist item	Location where item is reported
TITLE			
Title	1	Identify the report as a systematic review.	Title
ABSTRACT			
Abstract	2	See the PRISMA 2020 for Abstracts checklist.	Abstract
INTRODUCTION			
Rationale	3	Describe the rationale for the review in the context of existing knowledge.	Introduction
Objectives	4	Provide an explicit statement of the objective(s) or question(s) the review addresses.	Methodology

APPENDIX 1 (Continued)

Section and topic	Item #	Checklist item	Location where item is reported
METHODS			
Eligibility criteria	5	Specify the inclusion and exclusion criteria for the review and how studies were grouped for the syntheses.	Table 2
Information sources	6	Specify all databases, registers, websites, organisations, reference lists and other sources searched or consulted to identify studies. Specify the date when each source was last searched or consulted.	Table 3
Search strategy	7	Present the full search strategies for all databases, registers and websites, including any filters and limits used.	Table 3
Selection process	8	Specify the methods used to decide whether a study met the inclusion criteria of the review, including how many reviewers screened each record and each report retrieved, whether they worked independently, and if applicable, details of automation tools used in the process.	Screening
Data collection process	9	Specify the methods used to collect data from reports, including how many reviewers collected data from each report, whether they worked independently, any processes for obtaining or confirming data from study investigators, and if applicable, details of automation tools used in the process.	Screening
Data items	10a	List and define all outcomes for which data were sought. Specify whether all results that were compatible with each outcome domain in each study were sought (e.g. for all measures, time points, analyses), and if not, the methods used to decide which results to collect.	Data analysis
	10b	List and define all other variables for which data were sought (e.g. participant and intervention characteristics, funding sources). Describe any assumptions made about any missing or unclear information.	Data analysis
Study risk of bias assessment	11	Specify the methods used to assess risk of bias in the included studies, including details of the tool(s) used, how many reviewers assessed each study and whether they worked independently, and if applicable, details of automation tools used in the process.	Annotated bib (remove) Descriptive shown in App 1.
Effect measures	12	Specify for each outcome the effect measure(s) (e.g. risk ratio, mean difference) used in the synthesis or presentation of results.	n/a

APPENDIX 1 (Continued)

Section and topic	Item #	Checklist item	Location where item is reported
Synthesis methods	13a	Describe the processes used to decide which studies were eligible for each synthesis (e.g. tabulating the study intervention characteristics and comparing against the planned groups for each synthesis (item #5)).	n/a
	13b	Describe any methods required to prepare the data for presentation or synthesis, such as handling of missing summary statistics, or data conversions.	n/a
	13c	Describe any methods used to tabulate or visually display results of individual studies and syntheses.	n/a
	13d	Describe any methods used to synthesise results and provide a rationale for the choice(s). If meta-analysis was performed, describe the model(s), method(s) to identify the presence and extent of statistical heterogeneity, and software package(s) used.	n/a
	13e	Describe any methods used to explore possible causes of heterogeneity among study results (e.g. subgroup analysis, meta-regression).	n/a
	13f	Describe any sensitivity analyses conducted to assess robustness of the synthesised results.	n/a
Reporting bias assessment	14	Describe any methods used to assess risk of bias due to missing results in a synthesis (arising from reporting biases).	n/a
Certainty assessment	15	Describe any methods used to assess certainty (or confidence) in the body of evidence for an outcome.	n/a
RESULTS			
Study selection	16a	Describe the results of the search and selection process, from the number of records identified in the search to the number of studies included in the review, ideally using a flow diagram.	Figure 2
	16b	Cite studies that might appear to meet the inclusion criteria, but which were excluded, and explain why they were excluded.	n/a
Study characteristics	17	Cite each included study and present its characteristics.	Appendix 1
Risk of bias in studies	18	Present assessments of risk of bias for each included study.	Not completed
Results of individual studies	19	For all outcomes, present for each study: (a) summary statistics for each group (where appropriate) and (b) an effect estimate and its precision (e.g. confidence/credible interval), ideally using structured tables or plots.	Findings and Appendix 1

APPENDIX 1 (Continued)

Section and topic	Item #	Checklist item	Location where item is reported
Results of syntheses	20a	For each synthesis, briefly summarise the characteristics and risk of bias among contributing studies.	n/a
	20b	Present results of all statistical syntheses conducted. If meta-analysis was done, present for each the summary estimate and its precision (e.g. confidence/credible interval) and measures of statistical heterogeneity. If comparing groups, describe the direction of the effect.	n/a
	20c	Present results of all investigations of possible causes of heterogeneity among study results.	n/a
	20d	Present results of all sensitivity analyses conducted to assess the robustness of the synthesised results.	n/a
Reporting biases	21	Present assessments of risk of bias due to missing results (arising from reporting biases) for each synthesis assessed.	n/a
Certainty of evidence	22	Present assessments of certainty (or confidence) in the body of evidence for each outcome assessed.	n/a
DISCUSSION			
Discussion	23a	Provide a general interpretation of the results in the context of other evidence.	Findings
	23b	Discuss any limitations of the evidence included in the review.	Limitations
	23c	Discuss any limitations of the review processes used.	Limitations
	23d	Discuss implications of the results for practice, policy and future research.	Discussion and conclusion
OTHER INFORMATION			
Registration and protocol	24a	Provide registration information for the review, including register name and registration number, or state that the review was not registered.	Not pre-registered
	24b	Indicate where the review protocol can be accessed, or state that a protocol was not prepared.	n/a
	24c	Describe and explain any amendments to information provided at registration or in the protocol.	n/a
Support	25	Describe sources of financial or non-financial support for the review, and the role of the funders or sponsors in the review.	Declaration of interest statement
Competing interests	26	Declare any competing interests of review authors.	Declaration of interest statement
Availability of data, code and other materials	27	Report which of the following are publicly available and where they can be found: template data collection forms; data extracted from included studies; data used for all analyses; analytic code; any other materials used in the review.	Appendix 1 and data availability statement

Note: Page et al. (2021).

APPENDIX 2

List of studies included in the review ($N=75$)

Reference	Publication	Study location	Study methods	Approach	Level of education	Participants	# of participants	Approach to OSE
Adorjan and Ricciardelli (2019a)	Learning, Media and Technology	Canada	Focus group interviews	Quali	Secondary	Students	115	Safeguarding
Adorjan and Ricciardelli (2019b)	Young	Canada	Focus group interviews	Quali	Secondary	Students	115	Safeguarding
Agha et al. (2023)	Proceedings of the ACM on Human-Computer Interaction	USA	Interactive online bootcamp	Quali	Secondary	Students	21	Equipping/ safeguarding
Agosto and Abbas (2017)	New Media and Society	USA	Focus group interviews	Quali	Secondary	Students	98	Equipping
Andrews et al. (2020)	Journal of Public Policy and Marketing	USA	Interventions (with control group)	MM	Primary and secondary	Students	513	Equipping/ safeguarding
Bacak et al. (2022)	Computers in the Schools	USA	Interviews	Quali	Primary	Teachers	10	Equipping
Badillo-Urquiola et al. (2020)	Journal of Adolescent Research	USA	Retrospective analysis of student work	MM	Higher Education	Students	39	Equipping/ safeguarding
Berger and Wolling (2019)	Media and Communication	Germany	Survey	Quanti	–	Teachers	315	Equipping
Black et al. (2022)	Learning, Media and Technology	Australia	Focus group interviews and story writing methodology	Quali	Secondary	Students	33	Empowering
Boehmer et al. (2015)	Behaviour & Information Technology	USA	Survey	Quanti	Higher Education	Students	Study 1: 565, Study 2: 206	Equipping/ safeguarding
Boulton et al. (2016)	Cyberpsychology, Behaviour, and Social Networking	United Kingdom	Intervention (with control group)	Quanti	Primary	Students	295	Equipping

APPENDIX 2 (Continued)

Reference	Publication	Study location	Study methods	Approach	Level of education	Participants	# of participants	Approach to OSE
Buchanan et al. (2019)	Global Studies of Childhood	Australia	Focus group interviews	Quali	Primary	Parents and teachers	Parents: 9, Teachers: 14	Equipping
Buchanan et al. (2017)	E-Learning and Digital Media	Australia	Focus group interviews	Quali	Primary	Students	33	Equipping
Caton and Landman (2022)	British Journal of Learning Disabilities	United Kingdom	Interviews and focus group interviews	Quali	Secondary and higher education	Students, parents and teachers	Students: 27, Parents and teachers: 13	Equipping/ safeguarding
Chatlani et al. (2023)	International Journal of Child-Computer Interaction	USA	Focus group interviews	Quali	Secondary	Students	21	Empowering
Chiner et al. (2023)	British Journal of Learning Disabilities	Spain	Survey	Quanti	Primary and secondary	Teachers	208	Equipping/ safeguarding
Chiner et al. (2021)	International Journal of Disability, Development and Education	Spain	Survey	Quanti	Primary and secondary	Pre- and in-service teachers	582	Equipping/ safeguarding
Chou and Sun (2017)	Computers and Education	Taiwan	Questionnaire and interviews	MM	Primary and secondary	Teachers	505	Equipping
Choudhury and Choudhury (2023)	Psychology in the Schools	India	Semi-structured questionnaire	Quali	Secondary	School counsellors	30	Equipping
Cranmer (2013)	Learning, Media and Technology	England	Interviews	Quali	Primary, secondary and higher education	Students	13	Equipping
Cummings and Cleghorn (2022)	Journal of Children and Media	Trinidad and Tobago	Semi-structured interviews	Quali	Secondary	Students	51	Equipping

APPENDIX 2 (Continued)

Reference	Publication	Study location	Study methods	Approach	Level of education	Participants	# of participants	Approach to OSE
Edwards, Mantilla, et al. (2018)	Educational Practice and Theory	Australia	Diaries, newsletter article, and focus group interview	Quali	Early childhood education	Teachers	4	Equipping
Edwards et al. (2020)	International Journal of Environmental Research and Public Health	Australia	Participatory design approach	Quali	Early childhood education	Industry partners, teachers, parents and students	?	Equipping
Edwards, Nolan, et al. (2018)	British Journal of Educational Technology	Australia	Intervention (with randomised control group)	Quali	Early childhood education	Teachers and students	Teachers: 4, Students: 70	Equipping
Edwards et al. (2016)	Early Years	Australia	Interview schedule development	Quali	Early childhood education	Students	71	Equipping
El Asam and Katz (2018)	Human-Computer Interaction	United Kingdom	Questionnaire	Quanti	Primary and secondary	Students	2988	Equipping/ safeguarding
Ey and Cupit (2011)	Journal of Early Childhood Research	Australia	Focus group interviews	Quali	Primary	Students	57	Equipping
Hammond et al. (2023)	Information Communication and Society	United Kingdom	Semi-structured interviews	Quali	Primary, secondary and higher education	Educators	30	Equipping
Hanewald (2008)	Australian Journal of Teacher Education	–	Review	–	–	–	–	Safeguarding
Harrison (2022)	Pastoral Care in Education	–	Theoretical	–	–	–	–	Equipping
Hartikainen et al. (2019)	International Journal of Child-Computer Interaction	Finland	Workshops	Quali	Primary	Students	134	Equipping

APPENDIX 2 (Continued)

Reference	Publication	Study location	Study methods	Approach	Level of education	Participants	# of participants	Approach to OSE
Hernández-Martín et al. (2021)	Education and Information Technologies	Spain	Questionnaire	Quanti	Primary and Secondary	Students	595	Equipping/ safeguarding
Hina and Dominic (2016)	International Journal of Business Information Systems	Malaysia	Questionnaire	Quanti	Secondary	Students	380	Equipping
Hipsky and Younes (2015)	International Journal of Information and Communication Technology Education	USA	Questionnaire and interviews	MM	Higher Education	Faculty and staff	46 questionnaires and 6 interviews	Equipping
Hope (2010)	Australasian Journal of Educational Technology	United Kingdom	Interviews and observations	Quali	Primary and Secondary	Teachers and students	30 teachers and 63 students	Equipping
Kritzinger (2016)	South African Computer Journal	South Africa	Interviews	MM	Primary and Secondary	Teachers and principals	250 teachers and 29 principals	Safeguarding
Kritzinger (2017a)	Africa Education Review	South Africa	Survey	Quanti	Secondary	Students	503	Equipping/ safeguarding
Kritzinger (2017b)	South African Computer Journal	South Africa	Questionnaire	MM	Primary	Students	46	Equipping/ safeguarding
Kritzinger (2020)	Information (Switzerland)	South Africa	Survey	MM	Primary and Secondary	Schools	24	Equipping/ safeguarding
Livingstone and Haddon (2008)	Children and Society	European Union	Review	–	–	–	–	Equipping/ safeguarding
Lorenz et al. (2012)	Electronic Journal of E-Learning	Estonia	Survey and focus group interviews	Quali	Secondary	Students	192 surveys and 50 focus groups	Equipping
Mabitle and Kritzinger (2021)	International Journal of Information and Education Technology	South Africa	Survey	Quanti	Primary and Secondary	Teachers	109	Equipping

APPENDIX 2 (Continued)

Reference	Publication	Study location	Study methods	Approach	Level of education	Participants	# of participants	Approach to OSE
Macaulay et al. (2020)	Journal of Children and Media	United Kingdom	Questionnaire	Quanti	Primary	Students	329	Equipping
Martin et al. (2023)	TechTrends	USA	Interviews	Quali	Primary	Teachers	10	Equipping
Martin and Rice (2012)	Crime Prevention and Community Safety	Australia	Written submissions	Quali	–	Stakeholders	151	Equipping/ safeguarding
Masters and Barr (2009)	Knowledge Management and E-Learning	Australia	Online platform use analysis	Quanti	Primary	Students	160	Equipping/ safeguarding
McCarty et al. (2011)	Cyberpsychology, Behaviour, and Social Networking	USA	Survey	Quanti	Secondary	Students	139	Equipping
McDonald-Brown et al. (2016)	International Journal of Technology Enhanced Learning	New Zealand	Focus group interviews	Quali	Primary and Secondary	Students	39	Equipping/ safeguarding
McDonald-Brown et al. (2017)	E-Learning and Digital Media	New Zealand	Focus group interviews	Quali	Primary and Secondary	Students	39	Equipping/ safeguarding
Mishna et al. (2009)	Campbell Systematic Reviews	–	Systematic review	–	–	–	–	Equipping/ safeguarding
Moreno et al. (2013)	BMC Public Health	USA	Survey	Quanti	–	Teachers, clinicians, parents and adolescents	77 teachers, 111 clinicians, 72 parents, 96 adolescents	Equipping/ safeguarding
Nansen et al. (2012)	Journal of Children and Media	Australia	Multiple participatory methods	MM	Primary	Families and students	5 families	Equipping
Nicolaidou and Venizelou (2020)	Multimodal Technologies and Interaction	Cyprus	Intervention	Quanti	Primary	Students	48	Equipping
Ondrušková and Pospíšil (2023)	Contemporary Educational Technology	Czech Republic	Intervention	Quanti	Primary	Students	645	Equipping

APPENDIX 2 (Continued)

Reference	Publication	Study location	Study methods	Approach	Level of education	Participants	# of participants	Approach to OSE
O'Reilly and O'Neill (2008)	International Journal of Information and Communication Technology Education	Ireland	Survey	Quanti	Primary	Students	645	Equipping
Poblet et al. (2017)	Journal of Family Studies	Spain	Online platform use analysis, survey and focus groups	MM	Secondary	Students	940 survey, 60 focus group	Equipping
Polizzi and Harrison (2022)	Ethics and Information Technology	–	Theoretical	–	–	–	–	Equipping
Purnama et al. (2021)	Heliyon	Indonesia	Questionnaire	Quanti	Primary	Students	300	Safeguarding/ equipping
Pusey and Sadera (2011)	Journal of Digital Learning in Teacher Education	USA	Survey	Quanti	Higher Education	Pre-service teachers	318	Equipping
Rahman et al. (2020)	International Journal of Information and Education Technology	–	Systematic review	–	–	–	–	Equipping
Saglam et al. (2023)	IEEE Transactions on Education	–	Systematic review	–	–	–	–	Equipping
Saito et al. (2013)	Journal of Cases on Information Technology	Japan	Online platform use analysis, questionnaire and workshops	MM	Secondary	Students	79	Equipping
Schilder et al. (2016)	Journal of Youth and Adolescence	Belgium	Intervention	Quanti	Primary	Students	812	Equipping/ safeguarding

APPENDIX 2 (Continued)

Reference	Publication	Study location	Study methods	Approach	Level of education	Participants	# of participants	Approach to OSE
Shin and Lwin (2017)	New Media and Society	Singapore	Survey	Quanti	Secondary	Students	746	Safeguarding
Siyam and Hussain (2021)	TechTrends	United Arab Emirates	Policy analysis	Quali	–	–	–	Safeguarding/ equipping
Teimouri et al. (2018)	Sexuality and Culture	Malaysia	Survey	Quanti	Primary and Secondary	Students	420	Equipping/ safeguarding
Tick et al. (2021)	Electronics (Switzerland)	South Africa, Wales and Hungary	Survey	Quanti	Higher Education	Students	512	Equipping/ safeguarding
Tomczyk (2019)	Computers in the Schools	Poland	Survey	Quanti	Secondary	Teachers	421	Equipping
Touloupis and Athanasiades (2020)	Cambridge Journal of Education	Greece	Questionnaire	Quanti	Primary	Principals and teachers	542	Equipping/ safeguarding
Tsimtsiou et al. (2021)	International Journal of Adolescent Medicine and Health	Greece	Evaluation tool	Quanti	Secondary	Students	462	Equipping
Van der Hoven et al. (2013)	Journal of Media Literacy Education	Belgium	Survey	Quanti	Secondary	Students	638	Equipping
Van der Hoven et al. (2016)	Educational Technology Research and Development	?	Design based research	MM	–	–	–	Equipping
Vila-Counago et al. (2020)	Revista Iberoamericana de Tecnologias Del Aprendizaje	Spain	Explanatory sequential design	MM	Primary	Students	8	Safeguarding/ equipping
Walsh et al. (2022)	International Journal of Child-Computer Interaction	Australia	Framework development	–	–	–	–	Equipping
Wood and Atkinson (2015)	International Journal of Technologies in Learning	United Kingdom	Questionnaire and group discussion	MM	Higher Education	Pre–service teachers	~150	Safeguarding/ equipping