A policy document analysis of student digital rights in the Australian schooling context

Sean Groth
University of Newcastle

Erica Southgate
University of Newcastle

Abstract

Contemporary education is being undeniably shaped by datafication and while new algorithmic and automated decision making processes can have educational benefits, they also raise issues about children's digital rights and education policy responses to these rights. This study mapped how children's digital right to privacy and related human rights concepts are present in education policy documents of Australia's three largest state government departments of education. A children's rights coding framework was developed from the United Nation's "General comment No. 25 (2021) on children's rights in relation to the digital environment" and used to code the data set. Two levels of analysis were then undertaken. Level 1 involved code and subcode frequency analyses of concepts related to digital children's rights in policy documents. Level 2 was a descriptive qualitative analysis designed to understand how digital rights were expressed in policy. The study found that although all state government departments of education reflected some elements of children's digital rights, some states had a more complex, sustained, and public-facing commitment to expressing these in policy. The study concluded that Australian government departments of education should work towards providing more transparent public-facing policy on children's digital rights that can empower students and their families to make informed decisions within a rapidly shifting digital environment.

Introduction

Since 1990, Australia has been a signatory of the United Nations (UN) Convention on the Rights of the Child (CRC) (Australian Human Rights Commission, n.d.). The most widely ratified human rights treaty, the CRC comprises fifty-four Articles that set the foundation for children (those under 18 years of age) to have healthy and safe childhoods free from discrimination and ripe with opportunities for development (United Nations, 1989). Children's rights include the right to an education, to have access to and share reliable information, to be protected from information that may be damaging to them, and safeguards around privacy. The CRC stipulates that governments should make these rights comprehensible and available to children. In 2021, the CRC outlined the rights of the child in the digital age in a document titled "General comment No. 25 (2021) on children's rights in relation to the digital environment" [hereafter referred to as General Comment No. 25] (United Nations Committee on the Rights of the Child, [UNCRC], 2021). The document notes that the digital environment creates both opportunities and barriers for supporting children's rights.

The growth of the educational technology sector and increased integration of applications and platforms in school has seen a 'datafication' of education (Williamson et al., 2023). This is facilitated by "data infrastructures" which store, analyse, interpret, and display this information in pre-programmed ways (Gulson & Sellar, 2019). The intersection between the datafication of education and the growing realisation that children have rights in the digital domain is ripe for exploration. Using a novel framework derived from General Comment No. 25, this paper reports on a mapping of children's right to privacy and related digital rights concepts in publicly available policies of Australia's three largest government departments of education. The aim of the study was to explore how the digital rights of the child were reflected in publicly available Australian state government school education policy to understand implications for students and their families.

Literature Review

Datafication and Data Infrastructures

Data has been defined as "symbols that represent properties of objects, events and their environments" (Ackoff, 1989, p. 3). The collection and use of data has been around since the advent of schooling (Selwyn et al., 2021). Data has been defined as "symbols that represent properties of objects, events and their environments" (Ackoff, 1989, p. 3). The collection and use of data has been around since the advent of schooling (Selwyn et al., 2021). In computer science, Chen and colleagues (2009) define digital data as "computerized representations of models and attributes of real or simulated entities" (p. 13). Computing hardware company Lenovo (n.d.) provide this explanation of digital data:

> "Data is information that can be interpreted and used by computers. It is a collection of facts, such as numbers, words, measurements, observations or even just descriptions of things. In computing, data is typically stored electronically in the form of files or databases…. Computers only understand two types of data; binary code and character-based code. Binary code consists only of ones and zeros – which can be meaningful when put together in long, differentiated strings. Character-based code consists of letters, numbers, and symbols that humans recognize as part of an alphabet…" (para. 1 and 3).

Lehrer and colleagues (2002) stress that data are not characterised by intrinsic structures that allow humans to surmise answers. Rather it is the assumptions based in analytic approaches that must be used to draw inferences from data. Algorithms – rules that give a sequence of operations for solving specific types of problem (Hill, 2016), are used to draw inferences and provide answers to problems, which is being handled increasingly in an automated way.

Datafication refers to “the objective quantification of all kinds of human behaviour and sociality to enable real-time [digital] tracking, monitoring and predictive analysis” (Williamson, 2016, p. 124). Acceleration of datafication can be traced from the early 2000s with the growth of the internet which provided “big data” to develop powerful algorithms and cloud computing to support these. Ben-Porath and Harel Ben Shahar (2017) refer to the “5 Vs of big data – volume, variety, velocity, veracity, and value” (p. 243). Within schooling systems, big data can be (perpetually) generated through the myriad everyday demographic, welfare, medical, socioeconomic, and educational information about students and their families. This data is collected through mundane administration systems, assessment practices, and via data gathering and biometric tools, sensors integrated into digital devices and web browsers, and platforms and applications that are used for learning. Datafication, data infrastructures, and predicative and profiling outputs resulting from these continue to be driven by advances in artificial intelligence (AI).

AI in Education: Uses and Ethical Implications

AI has been described as “a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments” (Organisation for Economic Co-operation and Development, 2019). Machine learning (ML), an important subfield of AI, is the science of enabling machines to learn and behave in autonomous and often human-like ways by giving them data sets from the real world to improve learning over time (Faggella, 2020). Technically, ML is a complex field and there are certain ML approaches, such as artificial neural networks, that generate outputs that even the scientists who develop them cannot audit (Martin, 2019). Moreover, ML algorithms are often proprietary meaning that they are owned by government or the private sector and are not open for inspection. The technical complexity and/or proprietary interests has resulted in “black box” (something that is impenetrable or opaque) systems that have prompted concerns about transparency, accountability and privacy (Institute of Electrical and Electronics Engineers [IEEE], 2019).

The IEEE explains that “at least for the foreseeable future, developers [of autonomous and intelligent systems] will be unlikely to build systems that are guaranteed to operate as intended” (IEEE, 2019, p. 136). The history of AI is punctuated with issues of gender and racial bias and discriminatory outcomes (Akter et al., 2021), even where humans have been in-the loop (having oversight roles) but have overly trusted automated decision making (ADM) of AI (Kordzadeh & Ghasemaghaei, 2022), or have been complacent (Potasznik, 2023). The issue of ADM is further complicated by the complexity of algorithmic processes in the age of big data flows. As Wachter and colleagues (2021) explain:

> “Compared to human decision-making, algorithms are not similarly intuitive; they operate at speeds, scale and levels of complexity that defy human understanding, group and act upon classes of people that need not resemble historically protected groups, and do so

> without potential victims ever being aware of the scope and effects of automated decision-making" (p. 5).

Datafication, AI and automation have raised ethical and safety concerns especially when used with vulnerable populations such as children (Campolo et al., 2017). Calls for transparency of algorithmic processes and decision making, and clear processes for accountability regarding the use of AI in schools have been growing over the last few years (Southgate et al., 2019; European Commission, 2022).

The Digital Rights of the Child and General Comment No. 25

In 2021, the UNCRC published General Comment No. 25 which was the culmination of reports from UN member countries and recommendations from experts and key international stakeholders. It was informed by consultation with over 700 children from twenty-eight countries (Third & Moody, 2021). The consultation found that children wanted: access to affordable and reliable devices with connectivity and age-appropriate content; greater privacy protection, less surveillance, and more transparency; and protection from and remedy for discrimination, aggression and abuse experienced. The authors also stated that "80% of [children and young people] identified themselves as the 'servants' from whom others – primarily technology companies or digital content creators – profit financially" (Third & Moody, 2021, p. 100) and that this can be viewed as akin to economic exploitation.

Drawing on this consultation report, General Comment No. 25 captured the complexity of the digital environment and its challenges in the following way:

> "The digital environment… [includes] digital networks, content, services and applications, connected devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems, algorithms and data analytics, biometrics and implant technology… [It is] becoming increasingly important across most aspects of children's lives, including during times of crisis, as societal functions, including education… progressively come to rely upon digital technologies. It affords new opportunities for the realization of children's rights, but also poses the risks of their violation or abuse. During consultations, children expressed the view that the digital environment should support, promote and protect their safe and equitable engagement" (UNCRC, 2021, p. 1).

General Comment No. 25 has four rights-based principles: Non-discrimination; Best interests of the child; Right to life, survival and development, and; Respect for the views of the child. Briefly, *non-discrimination* addresses digital exclusion so that all children have equal, free, meaningful and safe access to the digital environment for leisure and learning. *Best interests of the child* stipulates that State parties' foremost consideration should be the optimal outcomes for children in the regulation, design, management and use of the digital environment and that there is transparency of decision making. The third principle recognises the role digital access and opportunities play in ensuring the child *right to life, survival and development*. The principle of *respect for the views of the child* highlights the need to develop and promote ways for children to advocate for their own rights, and that children should not be unnecessarily monitored in ways that violate their privacy or freedom of thought and opinion.

Study Setting

Australian schooling comprises government (public), Catholic and independent (private) schools. 65% of students attend a government school (Australian Bureau of Statistics [ABS], 2023). Each state and territory have a department or authority responsible for education that develop policy for government schools. This study focuses on the state government education departments of New South Wales (NSW), Queensland (QLD) and Victoria (VIC) which collectively make up 77% of enrolments in Australian government schools (ABS, 2023).

The Australian regulatory context for technology is disjointed. There is also currently no specific legislation to govern AI with the Privacy Act 1988 being under review for several years. The Australian Government Department of Industry, Science and Resources has released national, voluntary AI ethics principles and produced two discussion papers on AI regulation. There are national and state-based Commissions such as such as the Office of the Australian Information Commission and the Australian Human Rights Commission providing guidance on governance of technology, and in 2023, a national taskforce produced a draft National AI In Schools Framework. There is also an intergovernmental Safer Technologies for Schools (ST4S) initiative which provides privacy and safety advice on procurement. However, it is unclear exactly what this advice is and how it is implemented at a state government level. Much of the policy work (as opposed to guidance) surrounding the use of technologies in schools has fallen to state-based education departments for public schooling, diocese-based education administrators for Catholic schools, and principals in independent schools.

Study Approach and Design

The research aimed to explore how the digital rights of the child, as outlined in General Comment No. 25, were reflected in publicly available Australian state government school education policy. Both Vidovich (2001) and Cardno (2018) suggest that policy research can be broadly arranged into three categories. The first focuses on understanding influences within policy contexts; the second involves analysis of policy texts; and the third investigates the effects or 'consequences' of policy. Understanding decision-making processes within policy contexts around reasons for some education policy being publicly available while other policy remaining internal to education organisations (along with the consequences of this) are important areas for research. However, the present research was nestled within the category of policy as text to analyse the content of policy documents, and did not seek to draw conclusions on the context or consequences of policy, nor the underlying reasoning behind public versus non-public policy circulation. This decision was both pragmatic in terms of access to documents for analysis and connected to a human rights-based framing of ethical practice in public administration which stresses that people, including children, have a right to access, understand, participate in, and contest policies and regulations that can materially affect their ability to flourish.

The study was informed by an interpretivist epistemological framework to policy analysis that focused on mapping the frequency of key ideas, and how meaning and values are communicated through policy texts (Vidovich, 2001). Content analysis was utilised as "a set of procedures to make valid inferences from text… assessing the relative extent to which specified references, attitudes, or themes permeate a given message or document" (Prasad, 2008, p. 2).

As this was an analysis of publicly available policy documents, no ethics approval was required from a human research ethics committee.

Establishing the Data Set

Digital copies of publicly available policy documents were sourced from the respective online department of education policy libraries of the three states. The scope of the study did not extend to the collection of supporting standards, procedures, guidelines or adjunct explanatory documents. We acknowledge that there may be other relevant policies behind department firewalls or in other online repositories. The policy search occurred between the 10th – 24th of October 2022. Any policies added to, updated, or removed from policy libraries after these dates are not present in the study. The search identified 569 policy documents (NSW n = 97; QLD n = 38; VIC n = 434). Upon further investigation, documents that were rescinded, consolidated, did not exist when opened, or were publicly unavailable were excluded bringing the total to 553 policies (NSW n = 84; QLD = 38; VIC n = 431). Keyword searches were used to refine the data set. The first was a data/privacy-related word search using the keywords "Privacy", "Technology", "Online", "Protect", "Data", and "Digital". The search was not case sensitive or word-specific which allowed the search to capture words such as protect[ion] and digital[ly]. This refined the data set to 389 policies (NSW n = 48; QLD n = 30; VIC n = 311). A child-centric, non-case sensitive or word-specific search ("student[s]", "child[ren]", and "youth[s]") then occurred. Any documents that contained four or more technology or privacy-related keywords, but that did not contain any child-centric keywords were manually reviewed to create a data set of 325 policies (NSW n = 41; QLD n = 21; VIC n = 263). A further manual review revealed inappropriate inclusions which were removed from the data set. For example, the NSW '*Numeracy K-12*' policy contained the keywords "data" and "student", however upon manual review, it became clear that the two mentions of "data" referred to the curriculum content of "data analysis", and the use of "assessment data" to guide teaching programs, which were not relevant to the study. The final number of policies for analysis was 29 (NSW n = 5; QLD n = 6; VIC n = 18).

Coding Framework and Analysis

Prasad's (2008) concept of units of analysis and Cardno's (2018) inductive thematic data extraction and emergent categories process were used to develop the coding framework. Several steps were taken to achieve this. The first step used the word "privacy" as a unit of analysis within General Comment No. 25 which appeared thirty-six times. The second step involved understanding how the concept of privacy was explained within the context of the document (i.e. context units which is the meaning surrounding the idea). Step three involved identifying digital human rights concepts that were not specifically linked to the term "privacy" but were relevant to the digital rights of the child as reflected in the research literature. To consolidate categories into final codes, researcher 1 (Groth) met with researcher 2 (Southgate) over several meetings to discuss and interpret possible coding categories which resulted in 8 codes and 25 subcodes (Table 1). Two levels of analysis then occurred: *Level 1 analysis* consisted of a frequency count of the number of codes and subcodes numerically mapped to the policies; and, *Level 2 analysis* comprised a descriptive qualitative analysis of each policy document outlining its relationship to children's digital rights concepts.

Credibility of analysis was assessed through a recursive process of reviews (Vaismoradi et al., 2013) comprising inter-coder checking meetings where the coding of researcher 1 (Groth) was checked by researcher 2 (Southgate) with dialogue on areas of disagreement and consensus sought.

Table 1

Coding Framework

Subcode Code	Subcode a	Subcode b	Subcode c	Subcode d	Subcode e
1. Consultation process with children regarding privacy policy and supporting evolving capacities (Consultation)	N/A	N/A	N/A	N/A	N/A
2. Providing educational programmes and raising awareness of children's right to privacy (Awareness)	For children	For parents/caregivers	For the general public	N/A	N/A
3. The role of industry and the state in protecting children's right to privacy (Protections)	High cybersecurity standards for digital products/services and data handling	Demonstrating and embedding safety-by-design and privacy-by design principles	Addressing data breaches and provision of prompt and effective remedies	Industry compliance to implement regulatory frameworks with high ethical standards	N/A
4. Data and privacy regulatory principles (laws/regulations)	Specification of legitimate purpose for data collection	The principle of data minimisation and least privacy-intrusive practices	Mechanisms to prevent arbitrary or unlawful interference with children's privacy rights	N/A	N/A
5. Data/information privacy stipulations of state authorities (Privacy Stipulations)	Ensuring regular review and revision of policies and practices with consideration to equity and high ethical standards	Reference to child protection from online harm	Implementing child-friendly language and accessible formats for children to access their rights	Data consent and withdrawal of consent stipulation	N/A
6. Biometrics and automated processes (Biometrics/ADM)	Prohibiting practices that manipulate or interfere with children's right to freedom of thought and belief in a digital environment (i.e. Restrict automated and information filtering systems that affect or influence children's behaviour, emotions, or limit developmental opportunities)	Ensuring that ADM processes such as profiling and behavioural targeting do not result in discrimination for children	Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge	Ensure biometrics and other highly identifying information do not cause harm	Ensure products and services using embedded sensors and automated processes are subject to robust data protection and privacy standards
7. Governance processes/mechanisms (Governance)	Transparent data governance practices (e.g. what data is held, how/where is it held, who has access, for how long, for what purpose)	Independent oversight	Accountability (responsibility for governance)	Providing data owner's and parent's right to access, objection/complaint, contestability, rectification, and deletion	N/A
8. Digital safety (Safety)	Restrictions and content moderation for children (but not arbitrarily)	Exemption of parental consent and protection from family threats	N/A	N/A	N/A

Findings

NSW Department of Education Policy Analysis

Of the 97 public-facing policies located in the NSW Department of Education policy library, 5 met the criteria for explicitly reflecting the language or concepts of digital rights of the child, or 5.15% of the total number of policies identified. Level 1 analysis is summarised in Table 2. A single policy can make multiple references to subcodes within a code (e.g. Code 3 has three policies, but a total of four subcode references).

Table 2

Code and Subcode Frequency Mapping for NSW Department of Education Policy

			Distribution of Subcodes to Policy				
		Number of Policies	Subcode a	Subcode b	Subcode c	Subcode d	Subcode e
Distribution of Codes to Policy	1. Consultation	**1**	N/A*	N/A	N/A	N/A	N/A
	2. Awareness	**1**	0	1	0	N/A	N/A
	3. Protections	**3**	1	2	1	0	N/A
	4. Laws/Regulations	**3**	2	0	1	N/A	N/A
	5. Privacy Stipulations	**5**	5	1	0	0	N/A
	6. Biometrics/ADM	**0**	0	0	0	0	0
	7. Governance	**5**	1	1	5	3	N/A
	8. Safety	**1**	1	0	N/A	N/A	N/A

*N/A refers to no subcode for this category. This also pertains to Level 1 analysis tables for QLD and VIC.

Level 1 analysis revealed that only one policy referred to consultation with children regarding their right to privacy (Code 1) and only one policy described educating parents/caregivers about the right to privacy (Code 2). Code 3, the role of industry in protecting child privacy, appeared in three policies with a focus on cybersecurity, privacy preserving design of digital products and addressing data breaches, but not on industry compliance to regulation or ethical standards. Code 4 which was on regulation appeared in three policies which addressed the legitimate purpose of data collection and mechanisms to prevent arbitrary interference with privacy, but did not address least privacy-intrusive practices. Code 5, on the specifics of privacy stipulation by the state agency, was reflected in five documents with regular review mechanisms, and the prevention of online harm being the foci, but not the need for child-friendly accessible formats on this or data consent and its withdrawal. There was no mention of Code 6, biometrics, in any policy. Code 7 which was on governance processes appeared in five documents with most emphasis on accountability and complaints processes. Code 8, on digital safety, appeared in one policy with a focus on non-arbitrary restriction of content, but there was no document located that addressed exemption of parental consent for data collection to protect children from familial threats.

Level 2 analysis provided insight into how children's digital rights were framed in NSW policy text. Some examples of digital rights reflected in policies included the '*Complaints Handling*' policy which stated, "The department has a respectful and productive workplace culture where consumers, members of the community, and staff can raise their concerns directly" (p. 1), but did not reference children or how they might contest data privacy practices or have data rectified or deleted (Codes 4, 5, 7). The '*Social Media*' policy targeted staff and the standards that employees must uphold when using social media. It referenced the prohibiting of staff from posting information about students, "Employees must not post images, video and/or any identifying information about students" (p. 1) which prevents staff from unlawfully interfering with children's privacy rights (Code 4) on social media. The '*Information Security*' policy covered the cybersecurity standards and safety/privacy-by-design principles (Code 3) and stated necessities for "ensuring information is fit for purpose" (p. 1). However, this policy was generalised to all entities within the department and did not make specific mention to children or students. The policy that reflected the largest number of digital rights concepts was the '*Student Use of Digital Devices and Online Services*' policy which stressed consultation with students and parents/carers and school staff in developing school-level procedures for children's safe use of digital devices and online services (Codes 1, 2).

QLD Department of Education Policy Analysis

Of the 38 public-facing policies located in the QLD Department of Education policy library, 6 met the criteria for explicitly reflecting the language or concepts of digital rights of the child. This equated to 15.79% of the total number of policies identified. Level 1 analysis is summarised in Table 3.

Table 3

Code and Subcode Frequency Mapping for QLD Department of Education Policy

			Distribution of Subcodes to Policy				
		Number of Policies	Subcode a	Subcode b	Subcode c	Subcode d	Subcode e
Distribution of Codes to Policy	1. Consultation	**1**	N/A	N/A	N/A	N/A	N/A
	2. Awareness	**0**	0	0	0	N/A	N/A
	3. Protections	**4**	3	1	1	0	N/A
	4. Laws/Regulations	**2**	0	1	1	N/A	N/A
	5. Privacy Stipulations	**4**	4	1	2	0	N/A
	6. Biometrics/ADM	**0**	0	0	0	0	0
	7. Governance	**6**	1	2	4	2	N/A
	8. Safety	**1**	0	1	N/A	N/A	N/A

Level 1 analysis revealed that only one policy referred to consultation with children regarding their right to privacy (Code 1), and no policies described educating parents/caregivers, children or the general public about the right to privacy (Code 2). Code 3, the role of industry in protecting child privacy, appeared in four documents with cybersecurity, privacy preserving design of digital products and addressing data breaches being mentioned, but with no explicit allusion to industry regulation or ethical standards compliance. Code 4, on legal regulation, appeared in two policies which addressed data minimisation and preventing arbitrary interference with privacy, but no specifics on legitimate data collection. Code 5, on the explicit privacy stipulations of the state agency, was reflected in four policies with most emphasis on regular review of policy and practices to ensure ethics and equity, but with no mention of the need for child-friendly accessible formats or data consent and its withdrawal. There was no reference to Code 6, biometrics, in any policy. Code 7, on governance processes, appeared in six documents, with most emphasis on accountability and complaints processes. Code 8, on digital safety, appeared in one policy which was on exemption of parental consent for data collection to protect children under threat from their family, but lacked mention to content moderation.

Level 2 analysis provided insight into how children's digital rights were framed in QLD policies. The QLD policy library contained two '*complaints management*' policies split between general '*customer*' complaints and '*early childhood education and care*' complaints. They both contained information regarding the regular review of the policy and highlighted that children are given reasonable assistance to access their right to complaint (Code 5). They also described processes to request external reviews if complainants were dissatisfied with the internal outcome (Code 7), but did not explicitly address complaints about data collection and use. The '*ICT Asset Management Policy*' listed the roles and responsibilities for managing ICT assets which established a chain of accountability (Code 7). It also stated that 'all departmental ICT assets are risk managed and maintained in accordance with a defined lifecycle, industry best practice and manufacturer standards" (p. 1) indicating the application of high cybersecurity standards (Code 3). However, specific processes for the management of ICT assets were not covered in the policy and instead directed the reader to other documents or information, some of which were restricted to department employees. The '*Social Media Policy*' for employees stated, "Do not use or disclose on social media any confidential information or personal information obtained in your capacity as an employee of the department [including that pertaining to] images of employees, clients or students, without written consent" (p. 2). This is a similar mechanism to the NSW social media policy to prevent staff from infringing on children's privacy rights through social media (Code 4). The '*Information Security Policy*' commits to continuous review of standards and procedures to protect against information security risks (Code 3), and implements transparent governance mechanisms through, "A systematic and repeatable approach to information security risk" (p. 2) (Code 6). It applies "a risk-based approach to information security that maintains the confidentiality, integrity and availability of information" (p. 1) and safety-by-design principles through employee information updates and mandatory training (Code 3). The policy that covered the most concepts within the coding framework was the '*Child and Student Protection Policy*'. However, this policy was generalised to all forms of child and student protection and did not specifically focus on online protection.

VIC Department of Education Policy Analysis

Of the 434 public-facing policies located in the VIC Department of Education policy library, 18 met the criteria for reflecting the digital rights of the child, or 4.15% of the total number of policy documents identified. Level 1 analysis is summarised in Table 4.

Table 4

Code and Subcode Frequency Mapping for VIC Department of Education Policy

			Distribution of Subcodes to Policy				
		Number of Policies	Subcode a	Subcode b	Subcode c	Subcode d	Subcode e
Distribution of Codes to Policy	1. Consultation	**8**	N/A	N/A	N/A	N/A	N/A
	2. Awareness	**5**	4	5	3	N/A	N/A
	3. Protections	**13**	8	10	3	5	N/A
	4. Laws/Regulations	**8**	4	7	4	N/A	N/A
	5. Privacy Stipulations	**10**	3	4	4	5	N/A
	6. Biometrics/ADM	**2**	0	0	2	1	0
	7. Governance	**12**	6	2	6	5	N/A
	8. Safety	**6**	3	3	N/A	N/A	N/A

Level 1 analysis revealed that eight policies referred to consultation with children regarding their right to privacy. Code 2, describing educating children, parents/caregivers and the general public about the right to privacy was evident in five documents. Code 3, the role of industry in protecting children's privacy, appeared in thirteen documents with an emphasis on cybersecurity, privacy preserving design of digital products and industry compliance. Code 4, on legal regulation, appeared in eight policies with a focus on data collection minimisation to protect children's right to privacy. Code 5, on the explicit privacy stipulations of the state agency, was reflected in ten policies with comprehensive coverage across all subcodes. This was the only department of education to have policy addressing biometrics and automated processes (Code 6), but did not explicitly discuss prohibiting automated practices that interfere or influence children's development, preventing discrimination, or robust standards for embedded sensors and automated processes. Code 7, on governance processes more generally and specific to digital rights, were mentioned in twelve policies with coverage across all subcodes. Code 8, on digital safety, appeared in six policies and across both subcodes related to content moderation and exemption of parental consent for data collection when a child is under threat from family.

For level 2 analysis, some of the most relevant VIC policies to children's digital rights are discussed below. The '*CCTV in Schools – Installation and Management*' policy was one of the two policies that made reference to Code 6. This policy suggested that a CCTV privacy notice must be employed to "explain the purpose of the CCTV system… provide the location of CCTV cameras (either by listing the locations or providing a map)… explain how to request a record of any footage… provide a link to this policy for further information on how the school may use the CCTV system and who may access the footage" (p. 5). In addition to this, the policy described the use of easily understood (i.e. child-friendly) signage (Code 5), the right to access and complain about CCTV surveillance (Code 7), the optional consultation process that principals can undertake when considering digital surveillance (Code

1), and transparent (Code 7), least privacy intrusive practices (Code 4). The '*Cybersecurity and Responsible Use of Digital Technologies*' policy covered consultation with students (Code 1) regarding current technologies and relevant issues, provided educational information for students and parents on how to stay safe online and appropriate use of digital technology (Code 2), and schools adhering to safety-by-design and high cybersecurity standards (Code 3). Consideration was also given to transparent governance practices when introducing new devices or services (Code 7) and whether data consent is required when that application handles personal information (Code 5). The '*Digital Learning in Schools*' policy acknowledged the evolving capacities of children (Code 1), "The eSafety commissioner separates its child friendly guidance into children (6 to 11) and young people (12 to 18) reflecting their ability to make informed choices as they get older" (p. 13), along with the need to moderate online content for safety purposes (Code 8) and that "Students at primary school are less able to discern malicious and unsafe behaviour online… tighter restrictions should be placed on [these] students" (p. 13). Minimising children's risk of online harm was also mentioned (Code 5).

The '*Information Security – InfoSafe*' policy made generalised comment on raising awareness of information security (Code 2) to, "Establish and maintain an InfoSafe culture by promoting this policy and through ongoing conversations" (p. 2). High cybersecurity standards and safety-by-design principles (Code 3) were once again established, along with schools' requirements to promptly, "report any potential or confirmed information security incidents" (p. 3). This policy also required the VIC Department of Education and schools to ensure that industry suppliers adhered to set standards when providing new ICT systems (Code 3), "Ensure the security of new systems and the suppliers who provide them… meet Information Security and ICT security requirements" (p. 6). The '*Privacy and Information Sharing*' policy covered eighteen out of twenty-five subcodes which was the most subcodes referenced by a single policy. This policy had a section on biometric information (Code 6) and stipulated that "Schools must consult with the Department's Privacy team and their school community when considering using technologies that use biometric information. This will help schools to determine if the intended benefit of using the biometric technology outweighs the risks…" (p. 26). The '*Social Media Use to Support Student Learning*' policy encouraged consultation with students (Code 1) on how social media could be used in an education setting stating, "Students should be actively involved in the decisions about which social media websites and applications are used, and how they are used… and should have the opportunity to actively shape their own education" (p. 4).

To summarise, the three state departments of education had, to varying degrees, addressed different aspects of the digital rights of the child, with all having information security policies and social media policies designed to protect child privacy and cybersecurity measures. They all also contained complaints policies, but not necessarily tailored towards data profiling, consent in relation to digital products, or automated data harvesting and decision making. Only one department (VIC) had public-facing policy which explicitly addressed biometrics and certain types of automated processing of data (CCTV/facial recognition) and managing the risks of such practices.

Discussion

Understanding where the digital rights of the child are made explicit in education policy is important as it is an exercise in testing transparency and accountability of governance. As the datafication of schooling accelerates, and AI-powered ADM begins to permeate into many facets of educational technology, there is a need for more robust policy consideration to the benefits of digital products for teaching and learning, but also their implications for human rights. Education authorities have a responsibility to guide pedagogical practice, help school communities understand new technologies and to raise awareness of digital rights for students and their families. This is part of a growing public interest into digital reform (Livingstone & Third, 2017) that necessitates a more transparent and accountable approach to the governance of technology.

Wyatt-Smith and colleagues (2019) point out that "educational systems… [struggle with] digital data rights, and how to advise parents, students, and teachers about the best ways in which to protect private and personal information" (p. 17). The present study has highlighted how three state departments of education (NSW, QLD, VIC) were at various stages of implementing public-facing policy on digital rights. All departments had policies addressing cybersecurity and online safety, social media and online safety, but only VIC provided public-facing policy that had a more multi-faceted approach to raising awareness of digital rights for students and their families, and (theoretically) engaging students in understanding these rights.

New, highly user specific types of data being collected such as biometric, trace, and geolocation data are at the forefront of ethical debate for digital rights (Southgate et al., 2019; Williamson, 2020). These forms of data are key to ADM, and specific to adaptive, predictive and profiling software that is being integrated into a range of educational products. In the study data set, only the VIC Department of Education had policy that dealt with biometrics. There is much more overt policy development required to address the harvesting of biometric data in schools, data which is highly identifiable and personal. Similarly, the analysis did not locate any policy that explicitly dealt with data harvesting from embedded device geolocators or sensors, or relating to ADM. In an era of big data harvesting and increasing discussion of smart classrooms, developing privacy preserving and cyber-safe policy on these aspects of technology should be a priority.

The use of data monitoring practices (sometimes called dataveillance) to observe children's behaviour, development and learning outcomes is a hotly debated topic (Lupton & Williamson, 2017). It is often difficult to identify and enforce the line between 'fit-for-purpose' yet minimal data collection, and that which crosses the threshold to infringe on children's right to privacy. Transparency around the contractual (procurement, data usage and management) relationships between departments of education and technology providers would facilitate school community dialogue and understanding about this issue and would make an appropriate addition to public-facing policy. Commercial-in-confidence arrangements often sit in tension with clear accountability processes, and it is no longer enough for government agencies to ask the public to trust that human rights are being defended, especially with vulnerable populations such as children in a rapidly evolving digital environment.

Contribution, Limitations and Future Directions

This study provided a snapshot of an evolving education policy context in the face of tensions between rapid technological advancement and human rights. It provided insights into where children's digital rights were dealt with in schooling policy and where work on defending these rights needs to occur. The study offered a unique child's rights-based framework for interpreting strengths and gaps in schooling policy, and while there are guidelines being developed around AI for example, these are yet to be translated in the policies that teachers, students and their families have access to so that they may be empowered to understand and contest aspects of datafication. The study was limited in that it only provided a public-facing policy perspective and only related to three Australian state government departments of education, albeit those that govern the bulk of students in government schools. The study was also limited to document analysis, did not cover enactment of policy, and was restricted solely to policy documents without adjunct documents. We also acknowledge there may be relevant policy documents sitting behind department firewalls and work going on behind-the-scenes to address the issues raised in the paper. However, understanding the rationale behind why some policy documents remain unavailable to the public is important and requires further investigation.

Future research should also include investigation into the understanding of the digital rights of the child by teachers and school executive staff, along with their perceptions of its manifestation in policy and enactment in both schools and government. Understanding the realities of digital governance in schools within a decentralised schooling system and a national context characterised by disjointed regulation with few legislative protections such as Australia offers a different perspective to other contexts with strong regulatory frameworks such as the European Union. Research is required on how policymakers understand children's digital rights and how they might enact engagement with school communities to formulate policy. The current review of the Australian Privacy Act (1988) will perhaps reorient school education policy towards greater privacy-preserving technologies and human rights protections. On a related point, research on the digital rights of teacher's within the technology rich environments of schools and school systems is urgently required.

Conclusion

Datafication continues to be a major driving force behind the reshaping of contemporary education. There is attention being paid to the potential benefits heralded by AI and ADM such as adaptive and personalised learning. However, there is also ongoing global concern about human rights in the digital environment, including the digital rights of the child. Schooling policy is a vital component of governing technology to uphold children's rights, especially in national contexts of evolving or disjointed regulation of technology. Understanding how schooling policy omits or reflects children's digital rights is an important step to ensuring responsible, transparent and accountable governance of schooling systems, and to promote genuine engagement with students and their families to navigate the future of technology in education.

Declarations

Funding/Competing interests – No funding was acquired for this study and there are no competing interests to declare.

References

Ackoff, R. (1989). From data to wisdom. *Journal of Applied Systems Analysis*, *16*(1), 3-9. Retrieved September 7, 2023, from https://faculty.ung.edu/kmelton/Documents/DataWisdom.pdf

Akter, S., McCarthy, G., Sajib, S., Michael, K., Dwivedi, Y. K., D'Ambra, J., & Shen, K. N. (2021). Algorithmic bias in data-driven innovation in the age of AI. *International Journal of Information Management*, *60*, 102387. https://doi.org/10.1016/j.ijinfomgt.2021.102387

Australian Bureau of Statistics. (2023, February 15). *Schools.* https://www.abs.gov.au/statistics/people/education/schools/latest-release

Australian Human Rights Commission. (n.d.). *About children's rights.* https://humanrights.gov.au/our-work/childrens-rights/about-childrens-rights

Ben-Porath, S., & Harel Ben Shahar, T. (2017). Introduction: Big data and education: ethical and moral challenges. *Theory and Research in Education, 15*(3), 243-248. https://doi.org/10.1177/1477878517737201

Campolo, A., Sanfilippo, M., & Crawford, K. (2017). *AI now 2017 report*: AI Now Institute. Retrieved September 7, 2023, from https://ainowinstitute.org/publication/ai-now-2017-report-2

Cardno, C. (2018). Policy document analysis: A practical educational leadership tool and a qualitative research method. *Educational Administration: Theory & Practice, 24*(4), 623-640. https://eric.ed.gov/?id=EJ1305631

Chen, M., Ebert, D., Hagen, H., Laramee, R. S., Liere, R., Ma, K. L., Ribarsky, W., Scheuermann, G., & Silver, D. (2009). Data, information, and knowledge in visualization. *IEEE Computer Graphics and Applications, 29*(1), 12-19. https://doi.org/10.1109/MCG.2009.6

European Commission (2022). *Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators*. Retrieved September 7, 2023, from https://op.europa.eu/en/publication-detail/-/publication/d81a0d54-5348-11ed-92ed-01aa75ed71a1/language-en

Faggella, D. (2020, February 26). *What is machine learning?* https://emerj.com/ai-glossary-terms/what-is-machine-learning/

Gulson, K., & Sellar, S. (2019). Emerging data infrastructures and the new topologies of education policy. *Environment and Planning D: Society and Space, 37*(2), 350-366. https://doi.org/10.1177/0263775818813144

Institute of Electrical and Electronics Engineers. (2019). *Ethically aligned design.* Retrieved September 7, 2023, from https://standards.ieee.org/industry-connections/ec/ead-v1/

Kordzadeh, N., & Ghasemaghaei, M. (2022). Algorithmic bias: review, synthesis, and future research directions. *European Journal of Information Systems, 31*(3), 388-409. https://doi.org/10.1080/0960085X.2021.1927212

Lehrer, R., Giles, N., & Schauble, L. (2002). Data modeling. In R. Lehrer & L. Schauble (Eds.). *Investigating real data in the classroom: expanding children's understanding of mathematics and science* (pp. 1–26). Teachers College Press.

Lenovo. (n.d.). *What is data in computing?* Retrieved November 10, 2023, from https://www.lenovo.com/us/en/glossary/data/?

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society, 19*(5), 657-670. https://doi.org/10.1177/1461444816686318

Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society, 19*(5), 780-794. https://doi.org/10.1177/1461444816686328

Martin, K. (2019). Ethical implications and accountability of algorithms. *Journal of Business Ethics, 160*(4), 835-850. https://doi.org/10.1007/s10551-018-3921-3

Organisation for Economic Co-operation and Development. (2019, May 22). *Recommendation of the council on artificial intelligence.* Retrieved September 7, 2023, from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Potasznik, A. (2023, May 18-20). ABCs: Differentiating algorithmic bias, automation bias, and automation complacency. *In 2023 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS) (pp. 1-5).* IEEE.

Prasad, D. (2008). Content analysis: A method of social science research. In D. K. L. Das (Ed.), *Research Methods for Social Work* (pp. 174-193). Rawat Publications. https://doi.org/10.13140/RG.2.1.1748.1448

Selwyn, N., Pangrazio, L., & Cumbo, B. (2021). Attending to data: Exploring the use of attendance data within the datafied school. *Research in Education, 109*(1), 72-89. https://doi.org/10.1177/0034523720984200

Southgate, E., Blackmore, K., Pieschl, S., Grimes, S., McGuire, J., & Smithers, K. (2019, August 13). Artificial intelligence and emerging technologies in schools: Research report. Retrieved September 7, 2023, *Department of Education and Training, Australia.* https://apo.org.au/node/254301

Third, A. & Moody, L. (2021, March 3). *Our rights in the digital world: A report on the children's consultations to inform UNCRC General Comment 25.* 5Rights Foundation and Western Sydney University. Retrieved September 7, 2023, from https://5rightsfoundation.com/uploads/OurRIghtsinaDigitalWorld-FullReport.pdf

United Nations. (1989, November 20). *Convention on the rights of the child.* https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

United Nations Committee on the Rights of the Child. (2021, March 2). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, *15*(3), 398-405. https://doi.org/10.1111/nhs.12048

Vidovich, L. (2001, December 2-6). *A conceptual framework for analysis of education policy and practices* [Paper presentation]. 2001 AARE Annual Conference, Association for Research in Education, Fremantle, WA, Australia, https://www.aare.edu.au/data/publications/2001/vid01267.pdf

Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review, 41*, 105567. https://doi.org/10.1016/j.clsr.2021.105567

Williamson, B. (2016). Digital education governance: data visualization, predictive analytics, and 'real-time' policy instruments. *Journal of Education Policy, 31*(2), 123-141. https://doi.org/10.1080/02680939.2015.103578

Williamson, B. (2020). Bringing up the bio-datafied child: scientific and ethical controversies over computational biology in education. *Ethics and Education, 15*(4), 444-463. https://doi.org/10.1080/17449642.2020.1822631

Williamson, B., Macgilchrist, F., & Potter, J. (2023). Re-examining AI, automation and datafication in education. *Learning, Media and Technology*, *48*(1), 1-5. https://doi.org/10.1080/17439884.2023.2167830

Wyatt-Smith, C., Lingard, B., & Heck, E. (2019, October 25). *Digital learning assessments and big data: implications for teacher professionalism*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000370940