Computer Law & Security Review: The International Journal of Technology Law and Practice

Education in a Datafied World: Balancing Children's Rights and School's Responsibilities in the age of Covid 19

--Manuscript Draft--

Manuscript Number:	
Article Type:	Full Length Article
Keywords:	data protection; children; school; education; General Data Protection Regulation; right to object; rights; learner data; surveillance capitalism; data processing
Corresponding Author:	Emma Nottingham University of Winchester UNITED KINGDOM
First Author:	Emma Nottingham
Order of Authors:	Emma Nottingham
	Caroline Stockman
	Maria Burke
Abstract:	The Covid 19 pandemic created a situation where online learning extended at speed. Schools have been hard-pressed to provide an education during a time when it has not been possible for most children to physically attend due to national lockdowns. The efficacy and efficiency of digital platforms made it possible for schools to fulfill their duties to provide an education. However, the urgency of the situation carried the risk that this was put in place without adequate consideration of the data protection risks from various online learning tools. Although the General Data Protection Regulation (GDPR) provides a framework of regulations and rights to protect users, the legal process is unwieldy to apply due to tensions in balancing the rights of the child learner with the public need to ensure that all children are provided with an education. This paper recommends that changes in digital schooling practices are needed so that children have a realistically possible way that their data protection rights can be enforced as well as a clarified and uniformed approach to support schools.

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

The research has been funded by **Human Data Interaction** A UK EPSRC Network. The organisation has not influenced the development or content of the article.

Education in a Datafied World: Balancing Children's Rights and School's Responsibilities in the age of Covid 19

The Covid 19 pandemic created a situation where online learning extended at speed. Schools have been hard-pressed to provide an education during a time when it has not been possible for most children to physically attend due to national lockdowns. The efficacy and efficiency of digital platforms made it possible for schools to fulfill their duties to provide an education. However, the urgency of the situation carried the risk that this was put in place without adequate consideration of the data protection risks from various online learning tools. Although the General Data Protection Regulation (GDPR) provides a framework of regulations and rights to protect users, the legal process is unwieldy to apply due to tensions in balancing the rights of the child learner with the public need to ensure that all children are provided with an education. This paper recommends that changes in digital schooling practices are needed so that children have a realistically possible way that their data protection rights can be enforced as well as a clarified and uniformed approach to support schools.

Keywords: data protection; children; school; education; General Data Protection Regulation; right to object; rights; learner data; surveillance capitalism; data processing

1. Introduction

This paper explores the legal and ethical implications of the use of digital technologies in the schooling environment. It expresses concern that the use of digital platforms in this context is not upholding children's rights and puts children at risk of unnecessary, unethical and potentially harmful data processing. This paper acknowledges that data protection regulation exists to protect individuals in the digital world but explains that, with the increased use of digital platforms for school learning, there exists a tension between the protections offered under law and the reality of a digitised and connected learning environment. This presents a confusing and potentially hazardous path for the child, their parents and the school to navigate. Although schools act lawfully, the data processing that occurs when digital platforms are used can put children at risk. There may be no alternative option for a child who wants to, and must by law, receive an education, but to accept the invasive data practices now commonplace. The provision of alternatives is also logistically challenging for schools.

Existing literature has expressed concerns about the protection of children in the online world.[1] However, there is less literature exploring the nuances of the schooling context.[2] This paper seeks to capture some of the specific complexities facing the child and the school when digital platforms are

[1] For example, Marion Oswald, Helen James and Emma Nottingham, 'The not-so-secret life of five-year-olds: legal and ethical issues relating to disclosure of information and the depiction of children on broadcast and social media' (2016) 8(2) Journal of Media Law 198–228; Marion Oswald, Helen James, Emma Nottingham, Rachael Hendry, Sophie Woodman, 'Have 'Generation Tagged' Lost Their Privacy? A report on the consultation workshop to discuss the legislative, regulatory and ethical framework surrounding the depiction of young children on digital, online and broadcast media' (2017, British and Irish Law and Technology Association) <https://cris.winchester.ac.uk/ws/portalfiles/portal/356432/826826_Oswald_GenerationTagged_original.pdf> accessed 21 April 2021; Emma Nottingham, 'Dad! Cut that Part Out!' Children's Rights to Privacy in the Age of 'Generation Tagged': sharenting, digital kidnapping and the child micro-celebrity' in Jane Murray, Beth Blue Swadener and Kylie Smith (ed) *The Routledge International Handbook of Young Children's Rights* (Routlegde 2019); Veronica Barassi, *Child Data Citizen How Tech Companies Are Profiling Us from before Birth* (MIT Press 2020).

[2] For some examples see, Marko Teräs, Juha Suoranta, Hanna Teräs1 and Mark Curcher, 'Post-Covid-19 Education and Education Technology 'Solutionism': a Seller's Market (2020) 2 Postdigital Science and Education 863–878; David Buckingham, 'Epilogue: Rethinking Digital Literacy: Media education in the age of digital capitalism' (2020) 37 Digital Education Review 230-239.

used for learning. It argues that the justifications for relying on digital platforms for school learning are not always morally tenable or ethically appropriate. Greater awareness and education are needed so that children can be empowered to exercise their rights and be active agents over their own data. Parents need reassurance that online platforms are not exposing their children to unnecessary risks and feel able to assist children in exercising their right to object,[3] without fear of their child's education being compromised. Schools should be supported to ensure that they can provide online learning in a way that is safe and transparent and ensures that children are not put at unnecessary risks due to the invisibility of data processing and the subsequent harms that may occur in future as a result.

The first section of this paper contextualises the digital schooling environment. It explains that unethical data practices are happening via school learning due to the increased reliance on digital platforms and suggests that this is not morally appropriate. The second section addresses the legal position. It emphasises a fundamental tension between the child's right to object under Article 21 of the UK GDPR and the justifications of 'public task' and 'legitimate interest' under Article 6(1)(e) and (f), which schools can reasonably rely on to defend their digital learning practices.[4] It is suggested that this leaves ample space for third party companies to undertake unethical data processing of children without any negative legal consequences. This leaves children, parents and schools with limited opportunity for digital resistance, if any. The third section considers the development of children's rights in the digital world. It acknowledges that recent efforts to improve the recognition of children in this context are positive steps forward, including the launch of the UN Committee's General Comment No. 25 on children's rights in relation to the digital environment.[5] However, it emphasises that complexities of digital schooling need to be specifically addressed if the requirements of the General Comment are to be fully realised. This paper concludes by making key recommendations for the way forward.

Although this paper is primarily focused on the UK, it intends to have an international reach, as the tensions highlighted are applicable to children worldwide. This is especially significant in light of the novel challenges to school learning presented by the Covid-19 pandemic which forced millions of children into digital schooling. This paper therefore aims to put a spotlight on the unwarranted data-intrusive norms that have developed in the school education system prior to and during this time. It intends to draw the attention of law and policymakers to the legal discrepancies and the cultural challenges which allow pervasive data practices to exist in day-to-day learning. This is an issue of national and global priority for which development in law, policy and practice is needed.

2. Digital Learning in Context

The collection of children's data by schools is not a new practice and there is value in recording information about children in the schooling context. For instance, schools record data on a child's learning progress, how they compare to their peers as well as grades and feedback. Schools also record more sensitive data, such as attendance records, notes on personal difficulties, family circumstances, health conditions and learning differences. As online technology has developed, there has been more opportunity to improve the effectiveness of data collection through the integration of digital systems in schooling environments. For example, some schools take children's fingerprints on their first day, which can then be used to make 'fingerprint payments' for school lunches. A school building might be equipped with security cameras, electronic keycards can log when a door has been opened, and attendance apps can enable geolocation on school grounds.

[3] Article 21 UK General Data Protection Regulation.

[4] n.b. these provisions are the same in the EU General Data Protection Regulation.

[5] UN Committee on the Rights of the Child, General Comment No. 25 on children's rights in relation to the digital environment, CRC/C/GC/25 (2021) <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t> accessed 21 April 2021.

The influx of digital platforms in the modern-day school learning environment has therefore led to vast amounts of data being collected about children. 'The system' knows what children have eaten, which library book a child is borrowing, where in the school they are and where, according to their timetables, they should be going next. Simply being enrolled in school exposes children to data collection. As indicated above, digital tools can be extremely useful in enhancing and supporting children's education. For example, Holloway has suggested that data collection and analytics can help to personalise children's learning, increasing support where needed and maximising opportunities.[6] But this must be balanced against ethical concerns over *inter alia* the surveillance of children, their right to privacy and potential risks associated with data processing.[7]

Facial recognition software has also been developed for use in digital learning contexts.[8] Andrejevic and Selwyn have indicated that systems can take advantage of existing school practices of collecting photographs of children's faces for student records.[9] These can be used, for example, for accessing online content of courses,[10] authenticating the user,[11] or to confirm the identity of a student taking an online exam and confirming their presence for the exam duration.[12] Facial recognition software has also become a tool for monitoring student emotion and attention to detect learner engagement.[13] For example, it has been reported that some schools in China have systems which scan the room every 30 seconds to analyse student's emotions and behavior.[14] A start-up company in Hong Kong was reported to have developed a facial recognition software, known as '4 Little Trees', which recognises muscle movements in the face to determine emotions.[15] It also tracks how long a student takes to answer questions. It was considered to have been especially helpful for teachers during the Covid-19 pandemic for reading student's emotions.[16] However, this type of technology raises questions for fundamental human rights and freedoms of users, including both teachers and learners, as well as the more general concerns about data bias within AI systems, such as biased data regarding what it means to 'look engaged'.[17]

---

[6] Donnell Holloway, 'Surveillance capitalism and children's data: the Internet of toys and things for children' (2019) 170(1) Media International Australia 27–36, 32; Department for Education, 'Realising the potential of technology in education: A strategy for education providers and the technology industry' (2019) 14 <https://www.gov.uk/government/publications/realising-the-potential-of-technology-in-education> accessed 21 April 2021.

[7] David Buckingham, 'Epilogue: Rethinking Digital Literacy: Media education in the age of digital capitalism' (2020) 37 Digital Education Review 230-239; Neil Selwyn 'What's the Problem with Learning Analytics?' (2019) 6(3) Journal of Learning Analytics 11-19; Alan Rubel and Kylie M L Jones, 'The Temptation of Data-enabled Surveillance: Are Universities the Next Cautionary Tale?' (2020) 63(4) Communications of the ACM 22-24.

[8] For further discussion see, Mark Andrejevic and Neil Selwyn, 'Facial recognition technology in schools: critical questions and concerns' (2020) 45(2) Learning, Media and Technology 115-128.

[9] ibid, 120.

[10] Mark Andrejevic and Neil Selwyn, 'Facial recognition technology in schools: critical questions and concerns' (2020) 45(2) Learning, Media and Technology 115-128, 119.

[11] ibid, 119.

[12] Mark Andrejevic and Neil Selwyn, 'Facial recognition technology in schools: critical questions and concerns' (2020) 45(2) Learning, Media and Technology 115-128, 119.

[13] For discussion see Mark Andrejevic and Neil Selwyn, 'Facial recognition technology in schools: critical questions and concerns' (2020) 45(2) Learning, Media and Technology 115-128.

[14] Nila Bala, 'The Danger of Facial Recognition in Our Children's Classrooms' (30 April 2020) <https://www.rstreet.org/2020/04/30/the-danger-of-facial-recognition-in-our-childrens-classrooms/> accessed 26 March 2021. For further discussion see, Jeremy Knox, 'Artificial intelligence and education in China' (2020) 45(3) Learning Media and Technology 298-311.

[15] Milly Cha, 'This AI reads children's emotions as they learn' (February 17, 2021) <https://edition.cnn.com/2021/02/16/tech/emotion-recognition-ai-education-spc-intl-hnk/index.html> accessed 23 March 2021.

[16] ibid.

[17] Bettina Berendt, Allison Littlejohn and Mike Blakemore, 'AI in education: learner choice and fundamental rights' (2020) 45(3) Learning, Media and Technology 312-324.

The process of learning itself has also become increasingly 'datafied' i.e., subjected to data processing. Article 4(2) of the UK GDPR defines data processing as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[18] Like many online platforms, digital learning platforms may expose the child user to risks of data processing by tracking learning activities and achievements or learning behaviour. Any data collected can then be passed to 'on sellers' and data brokers who can make money from selling the data. Berendt has explained that, data collected via classroom behaviour modelling apps, such as ClassDojo, may be taken into a different context and used to analyse a child's behaviour beyond the initially intended purpose.[19] This can take place without the consent of children or parents. Whilst many digital tools are presented to the user and the school as a benefit, to help them fulfill their educational aims and duties, it is the invisible data mining operations behind the scenes which dominate. 'Surveillance capitalism' is present in many contexts in which a child engages with the online world.[20] In recent years, scholars and children's rights advocates, including the Children's Commissioner for England and organisations such as the 5Rights Foundation,[21] have become increasingly concerned about the ungoverned space in which the online world operates, which has led to data processing being the underlying norm in software design. Design is based on economic imperative and engineers the platform for the purpose of increasing corporate profit and developing extractive economic practices, which encourage maximum user engagement for increased opportunities for data collection.[22] Software for schooling purposes is no exception. Much like other forms of data, 'learner data' is a lucrative commodity.

Free applications in particular pose a risk. As Buckingham has identified, 'if the service is free, then you are the product – or at least your data is the product that is being bought and sold'.[23] But even paid-for technologies, many of which are low-cost, adopt business models focused on the collection of consumer data. In 2017, it was estimated that 30 million children in the US were using Google Classroom apps like Gmail and Docs, and that Chromebooks accounted for more than half of the mobile devices shipped to schools.[24] In February 2020, the Attorney General of New Mexico filed a lawsuit against Google for unlawfully tracking children's data through free Chromebooks provided to schools through the company's G Suite for Education platform (which has since been rebranded as Google

[18] Article 4(2) UK GDPR.

[19] Donnell Holloway, 'Surveillance capitalism and children's data: the Internet of toys and things for children' (2019) 170(1) Media International Australia 27–36, 32.

[20] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

[21] Children's Commissioner, 'Growing up Digital A Report of the Growing Up Digital Taskforce' (January 2020) <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf> accessed 2 April 2021; Sudeshna Mukherjee and Sonia Livingstone, 'Children and Young People's Voices' (2020, Digital Futures Commission, 5Rights Foundation) <https://digitalfuturescommission.org.uk/wp-content/uploads/2020/10/Children-and-Young-Peoples-Voices.pdf> accessed 2 April 2021.

[22] Shoshana Zuboff, 'Webinar - Launch of general comment No. 25 on children's rights in relation to the digital environment' (5Rigthts Foundation, 24 March 2021) 2 <https://5rightsfoundation.com/in-action/webinar---launch-of-general-comment-no--25-on-childrens-rights-in-relation-to-the-digital-environment.html> accessed 21 April 2021.

[23] David Buckingham, 'Epilogue: Rethinking Digital Literacy: Media education in the age of digital capitalism' (2020) 37 Digital Education Review 230-239, 233.

[24] Natasha Singer, 'How Google Took Over the Classroom' *The New York Times* (New York, 13 May 2017) <https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html> accessed 2 April 2021.

Workspace).[25] Similarly, Zoom came under scrutiny for a series of data privacy problems,[26] including a data exchange with Facebook about Zoom user behaviours and device features, even when that user did not have a Facebook account.[27] Further, it was reported that, in the first month of the Covid-19 pandemic, the number of active users of Google Classroom doubled to 100 million.[28] It became a 'go-to' platform for many schools and was recommended as a high-quality educational platform.[29] In February 2021, when the number of active users was reported to be 150 million, it was announced that Google would increase its educational offering with various new tools and add-ons.[30] Yet the company has been under national scrutiny for data protection violations, having received four GDPR fines including three in 2020.[31] It is therefore clear that user engagement with digital processing is not solely for the individual's pedagogic gain, but means the child learner is becoming a data point for the benefit of underlying market forces.

Scholars have coined various terms to describe children who are growing up with digitally intrusive norms including 'Generation Tagged'[32], 'The Datafied Child'[33] and 'Child Data Citizen'.[34] Oswald, James and Nottingham have warned that society is in danger of accepting a privacy-intrusive norm.[35] Data-driven society has normalised pervasive and invisible collection, use and storage of personal data by proprietary technologies, run through digital capitalism strategies. Such norms have seeped into the world of children's schooling. Since the Covid-19 pandemic, these norms have become even more entrenched. The national lockdowns during this time, when only children of key workers could

---

[25] Natasha Singer and Daisduke Wakabayashi, 'New Mexico Sues Google Over Children's Privacy Violations' *The New York Times* (New York, 20 February 2020) <https://www.nytimes.com/2020/02/20/technology/new-mexico-google-lawsuit.html> accessed 27 March 2021.

[26] Danny Hakim and Natasha Singer, 'New York Attorney General Looks Into Zoom's Privacy Practices' *The New York Times* (New York, 30 March 2020) <https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html> accessed 2 April 2021.

[27] Zack Whittaker, 'Maybe we shouldn't use Zoom after all' (*TechCrunch*, 31 March 2020) <https://techcrunch.com/2020/03/31/zoom-at-your-own-risk/> accessed 2 April 2021.

[28] Nick Fleming, 'After Covid, will digital learning be the new normal?' *The Guardian* (London, 23 January 2021) <https://www.theguardian.com/education/2021/jan/23/after-covid-will-digital-learning-be-the-new-normal> accessed 26 March 2021; Gerrit De Vynck and Mark Bergen, 'Google Classroom Users Doubled as Quarantines Spread' Bloomberg: Technology' (*Bloomberg*, 9 April 2020) <https://www.bloomberg.com/news/articles/2020-04-09/google-widens-lead-in-education-market-as-students-rush-online#:~:text=%20Google%20Classroom%20Users%20Doubled%20as%20Quarantines%20Spread,spent%20years%20entrenching%20itself%20in%20schools%20More%20> accessed 6 April 2021.

[29] Ross Morrison McGill, 'Using Google Classroom during a Pandemic' (*@TeacherToolkit*, 11 April 2020) <https://www.teachertoolkit.co.uk/2020/04/11/google-classroom> accessed 6 April 2021.

[30] Sarah Perez, 'Google to roll out slate of over 50 updates for Classroom, Meet and other online education tools' (*TechCrunch*, 17 February 2021) <https://techcrunch.com/2021/02/17/google-to-roll-out-slate-of-over-50-updates-for-classroom-meet-and-other-online-education-tools/> accessed 31 March 2021.

[31] GDPR Enforcement Tracker <https://www.enforcementtracker.com/> accessed 16 April 2021.

[32] Marion Oswald, Helen James and Emma Nottingham, 'The not-so-secret life of five-year-olds: legal and ethical issues relating to disclosure of information and the depiction of children on broadcast and social media' (2016) 8(2) Journal of Media Law 198–228; Marion Oswald, Helen James, Emma Nottingham, Rachael Hendry, Sophie Woodman, 'Have 'Generation Tagged' Lost Their Privacy? A report on the consultation workshop to discuss the legislative, regulatory and ethical framework surrounding the depiction of young children on digital, online and broadcast media' (2017, British and Irish Law and Technology Association) <https://cris.winchester.ac.uk/ws/portalfiles/portal/356432/826826_Oswald_GenerationTagged_original.pdf> accessed 21 April 2021.

[33] Deborah Lupton and Ben Williamson, 'The datafied child: The dataveillance of children and implications for their rights' (2017) 19(5) New Media & Society 780-794.

[34] Veronica Barassi, *Child Data Citizen How Tech Companies Are Profiling Us from before Birth* (MIT Press 2020).

[35] Marion Oswald, Helen James and Emma Nottingham, 'The not-so-secret life of five-year-olds: legal and ethical issues relating to disclosure of information and the depiction of children on broadcast and social media' (2016) 8(2) Journal of Media Law 198–228, 199.

physically attend school, exacerbated the need to rely on digital forms of learning. Livingstone explained that children's lives became 'digital by default' overnight.[36] In the schooling context, this amplified the dependance of schools and learners on digital platforms to meet the child's right to be educated.[37]

The Covid-19 pandemic provided an opportunity for education and technology companies to boost product advertising to teachers and schools. Google, Microsoft, Amazon and Zoom quickly grew their educational services. This growth continued throughout the first year of the pandemic and it has been predicted that the Global EdTech Market could be worth $404 Billion by 2025.[38] Williamson, Eynon and Potter have stated that the pandemic provided profit-making opportunities, as well as opportunities for world leading technology corporations to have influence over education practices.[39] Commercial influences have therefore played a role in the normalisation of digital learning, and thus the normalisation of pervasive data processing that accompanies it. The rush to move to remote learning meant that there was little transparency about the risks and implications of data processing or consideration of the impact that this may have on a child's future. Digital dependency also meant that there was no alternative to learning through digital platforms that are potentially collecting and harvesting the data of its users. Acceleration in the use of digital technologies has taken place without open public debate, with little reassurance as to the safety of the platforms being used and with no consultation with parents or children themselves.

Children and parents are not necessarily aware of the presence of data processing within the schooling context or have considered how it might impact the future. Those who are aware may, quite understandably, wish to reject the practices of data processing. There are some contexts in which it might be possible. For example, a parent could opt not have a smart speaker in the home or ensure that their children do not play with app-connected toys. However, the likelihood is that those who are concerned will be resigned to the fact that that digital platforms are necessary for school learning, without considering the possibility of questioning whether there is an alternative. Livingstone, Lansdown and Third note that both children and adults are not hugely concerned about commercial use of their data, with the mindset that it 'is the only 'deal' on offer'.[40] Not only does this further contribute to the norm of pervasive data processing but also creates a norm in which children, parents and schools do not question unethical practices. This leaves children in a disempowered position; exploited for economic gain with little opportunity for challenge.

Data protection concerns in education had already been identified prior to the Covid-19 pandemic. In February 2020, the Information Commissioner's Office, the UK's independent regulator for data protection and information rights law, published a report following a compulsory audit of the Department for Education (DfE).[41] This was carried out following complaints made by the organisations

---

[36] Sonia Livingstone, 'Almost overnight, children's lives became digital by default. What have we discovered?' (*LSE Blog* 23 March 2021) <https://blogs.lse.ac.uk/covid19/2021/03/23/almost-overnight-childrens-lives-became-digital-by-default-what-have-we-discovered/> accessed 23 March 2021; Sonia Livingstone, 'Digital by default: the new normal of family life under COVID-19' (*LSE Blog*, 13 May 2020) <https://blogs.lse.ac.uk/parenting4digitalfuture/2020/05/13/digital-by-default/> accessed 23 March 2021.

[37] Articles 28 and 29 United Nations Convention on the Rights of the Child (UNCRC).

[38] 'Global EdTech Market to reach $404B by 2025 - 16.3% CAGR' (*Holon IQ*, 6 August 2020) <https://www.holoniq.com/notes/global-education-technology-market-to-reach-404b-by-2025/> accessed 16 April 2021.

[39] Ben Williamson, Rebecca Eynon and John Potter, 'Pandemic politics, pedagogies and practices: digital technologies and distance education during the coronavirus emergency (2020) 45(2) Learning, Media and Technology 107-114, 108.

[40] Sonia Livingstone, Gerison Lansdown, and Amanda Third, 'The Case for a UNCRC General Comment on Children's Rights and Digital Media' (*Children's Commissioner*, 2017) 20 <https://www.childrenscommissioner.gov.uk/publication/the-case-for-a-uncrc-general-comment-on-childrens-rights-and-digital-media/> accessed 16 April 2021.

[41] Information Commissioner's Office, 'Department for Education: Data Protection Report' (2020) <https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-

defenddigitalme and Liberty, with respect to the National Pupil Database.[42] The audit found that data protection was not being prioritised and that this had severely impacted the DfE's ability to comply with data protection laws. The ICO identified 'a high risk that data will not be processed in a compliant manner and could result in multiple data breaches or further breaches of legislation'.[43] In addition they made a total of 139 recommendations for improvement, with over 60% classified as urgent or high priority.[44] It was also identified that there were cultural barriers within the DfE regarding data protection such as a lack of importance placed on data protection in the development of policy and practice, reflected in the lack of resourcing afforded to the Data Protection Officer and the impact this has had on what is achievable.[45] It was also observed that the DfE had been lax in its approaches when providing advice and guidance on data protection matters. This included not providing sufficient privacy information for data subjects, not fulfilling data security obligations and limited data protection training for staff.[46] It was identified that there was a reliance on staff to become self-aware of regulations and polices with no follow up on whether these have been read or understood.[47] It was also recognised that Data Protection Impact Assessments (DPIAs) were not being carried out early enough or at all, meaning that data processing was taking place without this safeguard in place.[48] While schools act with the best intent, the alarming findings in the ICO audit indicate that a child or parent could, reasonably and understandably, prefer to opt out of digital education. However, as is explained in the next section, there are practical difficulties for a child or parent who wishes to do this, and it places schools in a logistically difficult position to provide alternatives while maintaining educational access.

3. Data Protection: The Legal context

Although data protection regulation already exists,[49] and there have been recent developments to improve safety for children in the online world,[50] this section recognises that the digital learning context presents problems which current legal regulations do not sufficiently address. This section explores the legal context in which the issues discussed in the first section operate. Namely the possible tension

audit-executive-summary-v1_0.pdf> accessed 19 March 2021. n.b. Section 146 of the Data Protection Act 2018 gives the Information Commissioner the power to carry out compulsory data protection audits.

[42] 'Statement on the outcome of the ICO's compulsory audit of the Department for Education' (7 October 2020) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/statement-on-the-outcome-of-the-ico-s-compulsory-audit-of-the-department-for-education/> accessed 19 March 2021.

[43] Information Commissioner's Office, 'Department for Education (DfE) Data protection audit report' (February 2020) 5 <https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf> accessed 6 April 2021.

[44] ibid 3.

[45] Information Commissioner's Office, 'Department for Education (DfE) Data protection audit report' (February 2020) 4 <https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf> accessed 6 April 2021.

[46] ibid.

[47] Information Commissioner's Office, 'Department for Education (DfE) Data protection audit report' (February 2020) 5 <https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf> accessed 6 April 2021.

[48] ibid.

[49] Data Protection Act 2018; UK General Data Protection Regulation.

[50] For example, the Digital Economy Act 2017 created a UK age verification regulator; the Online Harms White paper, is to lead to the Online Safety Bill, seeks to improve safety for children online. See Government response <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf> accessed 6 April 2021; Information Commissioner's Office, Age appropriate design: a code of practice for online services (September 2020) available at https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf> accessed 6 April 2021; UN Committee on the Rights of the Child adopted General Comment No. 25 on Children's Rights in the Digital Environment <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en> accessed 6 April 2021.

between a child (or parent), who wishes to disengage from digital learning platforms versus school obligations to provide an education, against the backdrop of a society that has accepted, albeit somewhat unknowingly, a ubiquitous data-intrusive norm. This section explains the existing rules on data protection in the UK as well as the legal duties and responsibilities upon schools. It demonstrates why the legal framework leaves children at risk of unethical data processing, and therefore exposed to possible harms in future. It suggests that the current legal framework creates an impasse in the digital learning context, whereby children have little choice but to accept the practice of data processing for the sake of meeting educational needs.

3.1 Learner Data

'Learner data', is used by the authors to refer to data about the learner which is processed digitally through the proprietary teaching and learning technologies used in a schooling environment. We suggest that 'learner data' can fall within the category of personal data in Article 4(1) of the UK GDPR. This defines personal data as,

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Article 5 of UK GDPR sets out six principles which regulate the processing of personal data including: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality. The UK GDPR also provides a number of individual rights including, the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and rights in relation to automated decision making and profiling. This affords personal data, and accordingly some forms of 'learner data', a certain amount of protection and increased individual power. However, despite the implementation of these improved data protection regulations, there have still been rule breaches and reports of unnecessary data processing for commercial purposes, such as the unethical practices by Google through its education tools.[51] Further, the individual exercise of rights has not been the main priority since the Covid-19 pandemic and there are practical difficulties with the reality of exercising GDPR rights in the schooling context. As was identified in the ICO's audit of the DfE, internal cultural barriers and attitudes have been preventing 'an effective system of information governance, which considers the rights and freedoms of data subjects against their own requirements for processing personal data to ensure data is processed in line with the principles of the GDPR.'[52] The ICO audit also showed that there was limited training in a range of aspects including individual rights.[53] The cultural challenges are discussed in further detail in section 5.

---

[51] Sarah Perez, 'Google to roll out slate of over 50 updates for Classroom, Meet and other online education tools' (*TechCrunch*, 17 February 2021) <https://techcrunch.com/2021/02/17/google-to-roll-out-slate-of-over-50-updates-for-classroom-meet-and-other-online-education-tools/> accessed 31 March 2021.

[51] 'YouTube fined $170m for collecting children's personal data' *The Guardian* (London, 4 September 2019) <https://www.theguardian.com/technology/2019/sep/04/youtube-kids-fine-personal-data-collection-children-> accessed 26 March 2021.

[51] Natasha Singer and Daisduke Wakabayashi, 'New Mexico Sues Google Over Children's Privacy Violations' *The New York Times* (New York, 20 February 2020) <https://www.nytimes.com/2020/02/20/technology/new-mexico-google-lawsuit.html> accessed 27 March 2021.

[52] Information Commissioner's Office, 'Department for Education: Data Protection Report' (2020) <https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf> accessed 6 April 2021.

[53] ibid.

3.1.1 The Right to Object

Article 21 of the UK GDPR provides that a child can normally exercise their right to object to data processing from the age of 13.[54] But the practical application of this right in the real-world schooling environment is problematic. Although children (or their parents) have the right to object, it is legally, socially, and ethically unclear how it should be handled in practice, by school stakeholders, when it comes to digital learning and teaching technologies. Parallel to this, local authorities have a duty to provide an education to all children who cannot attend school as per Section 19(1) of the Education Act 1996. Although this provision was not designed to respond to the educational needs of children during the Covid-19 pandemic, it is still applicable to the context of remote learning. A child's education rights are also protected by international conventions. Article 2, Protocol 1 of the European Convention on Human Rights provides that: 'No person shall be denied the right to education'. Similarly, Article 28 of the United Nations Convention on the Rights of the Child (UNCRC) states that 'State Parties recognise the right of children to education' and Article 29 of the UNCRC adds a framework outlining the aims of education.

Although individuals have an absolute right to object to the processing of their personal data for direct marketing purposes, the reality is that the right to object is not absolute in the context of digital learning platforms for schooling, even where they are intertwined with commercial data processing by third-party companies. The UK GDPR outlines what constitutes a lawful basis for processing, including where processing is necessary for 'public task' or there is a 'legitimate interest'.[55] If an organisation has a lawful basis for processing, then an individual will not be able to exercise their right to object. 'Public task' and 'legitimate interest' can include schooling, which is in the public interest and necessary by law. If a child exercises their right to object against the use of digital learning platforms, this will be weighed against the school's public duty to provide an education and the wider social interest in children being educated. The school will be required to undertake a balancing exercise to explore whether the there is a justification for overriding the child's right. The Information Commissioner's Office advises:

> If you are deciding whether you have compelling legitimate grounds which override the interests of an individual, you should consider the reasons why they have objected to the processing of their data. In particular, if an individual objects on the grounds that the processing is causing them substantial damage or distress (eg the processing is causing them financial loss), the grounds for their objection will have more weight. In making a decision on this, you need to balance the individual's interests, rights and freedoms with your own legitimate grounds. During this process you should remember that the responsibility is for you to be able to demonstrate that your legitimate grounds override those of the individual.[56]

In the schooling context, the UK GDPR framework makes it relatively straightforward for a school to override the interests of a child who is exercising their right to object. This is especially so in the age of Covid-19 where the public duty to educate children remained prevalent and physical attendance in school was not an option, other than for children of keyworkers. As indicated in the above quote, if a child exercises their right to object, a school will need to carry out a balancing exercise in which they weigh up individual interests with their legal obligations to ensure that children receive an education. In carrying out this balance, schools can quite legitimately override an individual child's interests due to their public duty to educate, despite pervasive data processing practices that may be taking place.

[54] Below the age of 13, the right to object will lie with those with parental responsibility. Some schools may adopt a practice of also seeking parental consent for children aged 13 and over.
[55] Article 6(1)(e) and (f) UK GDPR.
[56] Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)' (2017, updated 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/> accessed 6 April 2021.

However, the ICO audit identified 'an overreliance on 'public task' as the lawful basis for sharing data which is not always appropriate and supported by identified legislation'.[57] It also suggested that there is limited understanding of the requirements, assessment, and application of 'legitimate interest'. Correspondingly, it recognised that DPIAs have not included 'a justification for lawful basis or details of how it applies to each specific processing activity'.[58] Further, we suggest that the balancing exercise that needs to be undertaken by schools, should a child exercise their right to object, is unclear as there is no specific guidance on how this should be handled in the schooling context.

Although the right to object and the right to be educated are both available in principle, it is unlikely that a child can adequately exercise both rights within the current regulatory framework. Invoking these rights is unlikely to lead to protection from pervasive data-intrusive practices. In the digital learning context, the right to object appears to be symbolic as it is difficult for a child to become an active agent over this right. In the unlikely event that a child succeeds in exercising their right to object, it is unclear how this situation might pan out, for both the child and the school. For the child who refuses to engage in digital learning, is there a sufficient alternative? Will there be a risk of not getting an education at all? Will a child feel excluded by the education system, purely for having exercised their legal rights over a genuine concern? How will a child who digitally resists be perceived by their peers and teachers and will the school environment be well-equipped to support a child with this decision? These questions make clear that the exercise of the right to object in the digital learning context presents an array of logistical issues for schools.

3.1.2 Special Category Data

Special category data is generally considered to be the most sensitive type of data. This is outlined in the UK GDPR as including: personal data revealing racial or ethnic origin; personal data revealing political opinions; personal data revealing religious or philosophical beliefs; personal data revealing trade union membership; genetic data; biometric data (where used for identification purposes); data concerning health; data concerning a person's sex life; and data concerning a person's sexual orientation.[59] In the schooling context for example, the collection and use of a child's fingerprint for 'fingerprint payments' in the cafeteria is classed as special category data. Similarly, a child's health information or their photographic image will also fall under this category. We consider that 'learner data' can, in some instances, constitute special category data. For example, if facial recognition software is used as part of a digital learning platform or if the settings of a digital learning platform need to be altered in light of a child's disability or learning difference.

Article 9(2) of the UK GDPR lists the conditions for processing special category data. As per Article 9(2)(a), this will generally mean that explicit consent is required for the processing of this data.[60] For instance, if a child or parent has given their consent to the collection of fingerprint data then they can, should they wish, later withdraw that consent.[61] This will mean that the data can no longer be lawfully

---

[57] Information Commissioner's Office, 'Department for Education (DfE) Data protection audit report' (February 2020) <https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf> accessed 6 April 2021; Article 6(1)(e) of the UK GDPR maintains that data processing can lawfully take place if carried out for public task.

[58] Information Commissioner's Office, 'Department for Education (DfE) Data protection audit report' 4 (February 2020) <https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf> accessed 6 April 2021

[59] Article 9(1) UK GDPR.

[60] The age at which a child can give their own consent under the EU GDPR, is 16 years. However, in the UK, that age limit was lowered to 13 years by the Data Protection Act 2018. For children below the age of 13, the consent of a parent is needed.

[61] Alessandro Mantelero, 'Competitive Value of Data Protection: The Impact of Data Protection Regulation on Online Behaviour' (2013) 3(4) International Data Privacy Law 229; Orla Lynskey, 'Deconstructing Data

used and will need to be deleted. They can also entirely refuse to give their consent in the first place. The *Data Protection: Toolkit for Schools* states that if a pupil or their parent does not want to use the fingerprint scanner to pay in the cafeteria (or other biometrics processing), alternatives will be provided, such as paying with cash.[62] The school should not preclude the child from using the cafeteria services. However, the provision of alternatives in relation to digital learning platforms, such as providing students with hard copies of work, is not guaranteed by law or national guidance. This is likely to be down to the individual discretion of the school.

Article 9(2)(g) provides that special category data can be processed for 'reasons of substantial public interest'. This is likely to be the lawful basis most often used by a school when processing special category data via digital learning platforms. This indicates that if a school can justify the overarching educational benefit, then this can outweigh any individual data protection concerns as well as eliminating the need to seek explicit consent. Much like the situation with personal data outlined above, this leaves child learners in a difficult and disempowered situation, with no choice but to accept pervasive data processing practices so that they can receive an education.

Scholars outside of the education context have expressed dissatisfaction with public interest justifications. Rinik has argued that,

> Grand and rather vague notions of data sharing being in the 'public interest' and helping to 'serve the public good,' offered as public justifications for the growth of data sharing, may be seen as mere window dressing for the voracious appetite for easier access to more personal data by business and government, which is needed for continued economic growth.[63]

This concern is prevalent in the schooling context, where the public interest in providing an education to children has a clear and obvious benefit. Therefore, a school can reasonably provide well justified evidence as to why they are overriding an individual child's interests. However, this is not to say that schools are to blame. Schools may have little autonomy over the digital platforms they use. The rush to move to online education during the Covid-19 pandemic also made schools vulnerable to the advertising of large technology corporations who could step in to provide effective digital tools in the pedagogic sense, but who would have hidden agendas for profit-making via data processing. As a society, we need to consider whether the rights and obligations regarding education are enough to constitute reasons of 'substantial public interest' to the point of tipping the balance against individual rights of learners, leaving them exposed to unethical data processing practices by third parties.

3.1.3 Anonymised 'learner data'

We suggest that 'learner data' can also fall outside of the categories of personal data and special category data. This is because some digital learning platforms might collect data that has been fully anonymised and thus does not show the relationship between the data and the user. The UK GDPR does not apply to data that has been anonymised. Recital 26 explains that,

> …The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or

---

Protection: The "Added Value" of a Right to Data Protection in the EU Legal Order' (2014) 63(3) International and Comparative Law Quarterly 569.

[62] Department for Education, 'Data protection: a toolkit for schools Open Beta: Version 1.0' 26, 36 (August 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf> accessed 6 April 2021.

[63] Christine Rinik, 'Data trusts: more data than trust? The perspective of the data subject in the face of a growing problem' (2019) 34(3) International Review of Law, Computers and Technology 342-363, 343.

> to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Consequently, anonymised 'learner data' will not benefit from the protections provided to personal data outlined above. Rinik has suggested that there are two main difficulties with the application of Recital 26.[64] With reference to the work of the Law Commission,[65] she identifies that data controllers will attempt to preserve as much individual details about the user's characteristics as they can, whilst complying with anonymisation. She acknowledges that data is more valuable if it preserves the individual user's characteristics.[66] Further, she indicates concern in light of the fact that it is possible to use technology and recombine data sets in order to re-identify an individual's data that was previously considered to be anonymised.[67] These observations are relevant to the schooling context, where it may be that anonymised data collection could still leave a child exposed to unethical and unnecessary risks. A child in this situation will not be supported by the UK GDPR framework as it will not be relevant to seek the child's consent or make available the right to object. This adds to the socially disempowered position of the child in the digital schooling environment.

4. Development of Children's Rights in the Digital Learning Environment

In recent years there has been an increasingly growing movement towards the realisation of children's rights in the online world. Scholars and child rights organisations have expressed concerns about the exploitation of children for their data as well as infringements with fundamental rights such as the right to privacy.[68] In response, developments have been made to help recognise children's rights in the digital environment and increase the level of protection available as well as placing responsibility on organisations to adopt child-rights approaches to their digital designs and practices. This section considers the impact of these developments in the digital learning context and suggests that they constitute positive steps forward that might lead to some improvement for the safety of children using digital learning platforms. However, we maintain that there is still a need for improved regulations and guidance to address the specific challenges of the digital learning context outlined in this paper.

4.1 UK Developments

The UK Government has pledged its ambition to make the UK the safest place in the world to go online.[69] Ongoing legal and policy changes intend to ensure that children are better protected in the

---

[64] Christine Rinik, 'Data trusts: more data than trust? The perspective of the data subject in the face of a growing problem' (2019) 34(3) International Review of Law, Computers and Technology 342-363.
[65] Law Commission, *Data Sharing between Public Bodies: A Scoping Report* (Law Com No 351, 2014).
[66] Christine Rinik, 'Data trusts: more data than trust? The perspective of the data subject in the face of a growing problem' (2019) 34(3) International Review of Law, Computers and Technology 342-363, 347.
[67] Christine Rinik, 'Data trusts: more data than trust? The perspective of the data subject in the face of a growing problem' (2019) 34(3) International Review of Law, Computers and Technology 342-363, 347, referencing Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) Law, Innovation and Technology 40–81, 47 and Law Commission, *Data Sharing between Public Bodies: A Scoping Report* (Law Com No 351, 2014) para 1.111.
[68] For example see, Mariya Stoilova, Sonia Livingstone and Rishita Nandagiri, 'Children's data and privacy online Growing up in a digital age' (2019) <https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf.> accessed 28 April 2021; Veronica Barassi, *Child Data Citizen How Tech Companies Are Profiling Us from before Birth* (MIT Press 2020).
[69] Government Press Release, 'Making Britain the safest place in the world to be online' (2017) <https://www.gov.uk/government/news/making-britain-the-safest-place-in-the-world-to-be-online> accessed 28 April 2021.

digital age. Below, we examine whether recently established and proposed developments are effective for ensuring children's rights in the digital schooling context.

4.1.1 Department for Education Guidance

Since the digital world entered the realm of school education, the DfE has responded with various guidelines. For instance, the *Data protection: a toolkit for schools* was published in response to the GDPR.[70] This provides guidance to help schools develop policies and processes for data handling. Despite a comprehensive set of steps that schools can implement, the guidance leaves open the possibility of a lawful basis for the processing of data. We agree that reasons for lawful basis should exist in the school education context but are concerned that the public duty to educate and the child's right to be educated can be relied on too heavily, leaving children exposed to the risks of unethical data processing. The toolkit does not go far enough to close the gap by which third parties can monetise 'learner data'.

The outbreak of the Covid-19 pandemic prompted further guidelines. In April 2020, the DfE published *Guidance Safeguarding and remote education during coronavirus (COVID-19).*[71] The guidelines suggest that '[s]chools and colleges should continue to follow guidance on data protection and GDPR' and refer to the guidance in the *Data protection: a toolkit for schools* and from the ICO.[72] The DfE also published *Keeping Children Safe in Education (2020) Statutory guidance for schools and colleges*, which came into force on 1 September 2020. These reports include additional information and support to help schools and colleges keep children and young people safe online. Although they provide some important resources for improving children's online safety, very little is offered in the way of increased protection for children whose data is being monetised by third party corporations via digital learning platforms, which has become a more pressing concern during the Covid-19 pandemic. We argue that DfE guidance should do more to ensure that schools do not fall victim to the lure of free and easy-access digital learning platforms which, through the collection of data for educational reasons, are simultaneously harvesting the data of children for commercial gain. Further guidelines should ensure that individual data protection rights of child learners are given greater weight when balanced against reasons of 'substantial public interest', 'public task' and 'legitimate interest'. Educational rights and responsibilities are not enough of a justification to warrant exposing children to unethical data processing.

4.1.2 Age-Appropriate Design Code

The Data Protection Act 2018 (DPA) has encouraged the design of safeguarding measures for children. Section 123(1) of the Act required the Information Commissioner to develop a Code of Practice to improve standards of protection for children in the digital world. This led to the Age Appropriate Design Code which was published in September 2020, with a one year transition period for organisations to ensure compliance. The code applies to 'relevant information society services which are likely to be accessed by children'.[73] This includes a range of websites, programs, apps, social media sites, as well as online games, toys and connected devices. The aim of the code is to support compliance with the DPA and the GDPR, through setting out 15 standards, to act as a 'benchmark for the appropriate

[70] Department for Education, 'Data protection: a toolkit for schools Open Beta: Version 1.0' 26, 36 (August 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf> accessed 6 April 2021.

[71] Department for Education, 'Safeguarding and remote education during coronavirus (COVID-19)' (2020) <https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19> accessed 20 April 2021.

[72] ibid.

[73] Article 6(1)(e) and (f) UK GDPR.

protection of children's personal data',[74] which should be built into the design of services likely to be accessed by children. The code is said to incorporate the standards of the UNCRC including Article 3, the best interests of the child as the primary consideration.[75] It also endorses the use of default settings that are data minimisng and that children who choose to change these settings are supported with information, advice and guidance before they do so.[76] The ICO maintains that it will monitor compliance with the code through audits and complaints processes and take action to enforce data protection rules.[77] The code also suggests that organisations have their own systems of accountability and governance to observe compliance with data protection legislation.[78]

At the time of writing, the Age Appropriate Design Code is in its transition year for implementation. The impact that it will have in the schooling context is yet to be seen. The code does not specifically consider 'learner data' but the explanatory memorandum includes educational websites in their list of online platforms that will be covered by the code.[79] Therefore there may be some improvement to the digital schooling environment once the transition period has passed in September 2021. However, the code also emphasises that there can be a lawful basis for processing personal data and refers to Article 6 of the UK GDPR which includes 'public task' and 'legitimate interest'.[80] Similarly, it suggests that Article 9(2)(g),'substantial public interest', can be relied upon for the processing of special category data. As has already been discussed at 3.1.1 and 3.1.2, there are difficulties with schools relying on 'public task', 'legitimate interest' and 'substantial public interest' as a child's right to object or decline consent can be easily outweighed by a school's legal obligation to provide an education. This can leave a child subjected to unethical and unnecessary data processing, with no recourse but to resign themselves to the data-intrusive norm.

It is not yet clear whether the Age Appropriate Design Code will adequately respond to this specific complexity. If all host platforms are designed with child protection at the forefront in the first instance, then the need to exercise the right to object or decline consent will diminish, as will the tension between these rights and the legal obligation on the school to provide an education. However, there may continue to be difficulties with data protection enforcement especially as, on some occasions, technology companies might still profit from data breaches despite having to pay a hefty fine. Further, it is not clear whether the code will address the concerns outlined at section 3.1.3, about the collection of children's anonymous data.

4.1.3 Online Safety Bill

In April 2019, the Department for Digital, Culture, Media and Sport published the Online Harms White Paper.[81] A subsequent Government consultation response was published in December 2020.[82] The

---

[74] Information Commissioner's Office, Age Appropriate Design Code: a code of practice for online services' (2020) 23 <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf> accessed 6 April 2021.
[75] ibid 4.
[76] Information Commissioner's Office, Age Appropriate Design Code: a code of practice for online services' (2020) 23 <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf> accessed 6 April 2021.
[77] ibid 89.
[78] Information Commissioner's Office, Age Appropriate Design Code: a code of practice for online services' (2020) 84-87 <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf> accessed 6 April 2021.
[79] Explanatory memorandum to the Age Appropriate Design Code 2020 (11 June 2020) <https://www.gov.uk/government/publications/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020> accessed 6 April 2021.
[80] ibid 101-106.
[81] Department for Digital Culture, Media and Sport, *Online Harms White Paper* (White Paper, Cm 57, 2019).
[82] Department for Digital Culture, Media and Sport, *Online Harms White Paper: Full government response to the consultation* (White Paper, Cm 354, 2020).

proposals, including the implementation of a statutory duty of care owed by online host platforms to children, are consolidated in the Online Safety Bill.[83] Despite applying to many aspects of the digital environment which affect children, the education context is not included.

> The government will exempt services used internally by organisations, services managed by educational institutions that are already subject to regulatory or inspection frameworks (or similar processes) that address online harm, email and telephony providers, and services with limited user functionality.[84]

Concerns with the 'education exemption' have been highlighted in a report by the 5Rights Foundation, especially regarding the suggestion that services managed by educational institutions are already subject to regulatory or inspection frameworks.[85] They suggest that this does not reflect the reality that teachers and school children use online services that have not necessarily been put through school procurement or safeguarding procedures.[86] Further they state that,

> By characterising online harm in education settings as a safeguarding issue, the government has failed to consider that many EdTech providers do not offer fit for purpose security mechanisms on learning platforms or provide sufficient protections for children's data. It also outsources the cost of mitigating harm onto the education sector, which spends increasing amounts of money and hundreds of school hours on safeguarding issues that could be avoided.[87]

We agree that the justifications for excluding education from the Online Safety Bill is based on a misassumption about existing data protection practices in schools. The proposals appear to indicate that data protection in schools is already appropriately regulated and supported. But the reality is that greater consideration of the risks posed by digital learning technologies is needed as well as improved support for schools in giving more effective recognition of individual learners' rights.

4.2 International Instruments

The rights of children in the digital age have become a focal point at an international level and will be receiving increased protection and representation as a result of recent international instruments including the UN General Comment No. 25 on children's rights in relation to the digital environment, which confirms the application of the United Nations Convention on the Rights of the Child (UNCRC) in the online word, and the Council of Europe Guidelines on Children's Data Protection in an Education Setting. Although the UK is not bound by the provisions of the UNCRC and was in its transition year of leaving the European Union at the time of publication of the Council of Europe guidelines, these updates are worth examining.

4.2.1 UN General Comment No. 25 on children's rights in relation to the digital environment

The UNCRC sets out a framework by which states should provide specific protections to different aspects of children's rights. In 2014, the UN Committee on the Rights of the Child convened to discuss

---

[83] ibid.
[84] Department for Digital Culture, Media and Sport, *Online Harms White Paper: Full government response to the consultation* (White Paper, Cm 354, 2020) 12.
[85] 5Rights Foundation, 'Ambitions for the Online Safety Bill' (April 2020) 9 <https://5rightsfoundation.com/uploads/Ambitions_for_the_Online_Safety_Bill.pdf> accessed 23 April 2021.
[86] ibid.
[87] 5Rights Foundation, 'Ambitions for the Online Safety Bill' (April 2020) 9 <https://5rightsfoundation.com/uploads/Ambitions_for_the_Online_Safety_Bill.pdf> accessed 23 April 2021.

the implications of the convention in light of the digital age.[88] In 2017, the Children Commissioner's *Growing up Digital* report reviewed the UNCRC's provisions and suggested adjustments for the digital age.[89] The report called for a General Comment, which would include guidance on addressing the commercial design of digital technology, in order to better protect children's rights. This was subsequently developed into General Comment No. 25 on children's rights in relation to the digital environment and, in February 2021, was officially adopted by the UN Committee on the Rights of the Child. The General Comment was launched on 24 March 2021 at a webinar hosted by the 5Rights Foundation.[90] It confirms that the UNCRC now applies in the online world, including the schooling context. Therefore, the safeguards and support for children to be active participants and agents of their school learning should apply in the online world, just as they do for the offline world.

The UN General Comment No. 25 makes important points with regard the protection of children's data. With reference to the best interests of the child, it outlines that 'States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling'.[91] In relation to the context of schooling, it states that '[s]tandards for digital educational technologies should ensure that the use of those technologies is ethical and appropriate for educational purposes and does not expose children to violence, discrimination, misuse of their personal data, commercial exploitation or other infringements of their rights'[92] This is a welcome development in the field of digital schooling. We suggest that these provisions should be interpreted such that, in the school learning context, data should only be collected for reasons that relate to the child's education and have clearly defined and ethically justified retention periods. For example, data collection might be needed for submitting work and receiving feedback or for receiving lessons online when necessary, but this should not be intertwined with unethical third-party data processing. Children should be able to engage in digital learning in a way that is safe and transparent without the hidden presence of surveillance capitalism.

Despite the aforementioned words of the UN General Comment No. 25 being a positive development, we are concerned that there could still be tensions between the right to object or withdraw consent and the public duty to ensure that children are educated. The UN General Comment No. 25 suggests that State parties 'should further ensure the right of children to withdraw their consent and object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing.'[93] We agree that increased efforts in ensuring these individual data protection rights are necessary but this will only have a limited impact in the schooling context if these rights can virtually

---

[88] UN Committee on the Rights of the Child Report of the 2014 Day of General Discussion, 'Digital media and children's rights' (2014) <https://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf> accessed 21 April 2021.

[89] Children's Commissioner, 'Growing up Digital A Report of the Growing Up Digital Taskforce' (January 2020) <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf> accessed 2 April 2021

[90] 5Rights Foundation, 'Webinar - Launch of general comment No. 25 on children's rights in relation to the digital environment' (2021) <https://5rightsfoundation.com/in-action/webinar---launch-of-general-comment-no--25-on-childrens-rights-in-relation-to-the-digital-environment.html> accessed 21 April 2021.

[91] UN Committee on the Rights of the Child, General Comment No. 25 on children's rights in relation to the digital environment, CRC/C/GC/25 (2021) para 42 <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t> accessed 21 April 2021.

[92] ibid para103.

[93] UN Committee on the Rights of the Child, General Comment No. 25 on children's rights in relation to the digital environment, CRC/C/GC/25 (2021), para 72 <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t> accessed 21 April 2021.

always be outweighed by the legal obligation to educate and the child's right to be educated. We consider that public duties to educate and the child's right to be educated should not be at odds with the need to keep children free from pervasive data processing practices. As has been stated by UNICEF, children's rights should work together and no one right is more important than the other.[94]

4.2.2 Child Rights Impact Assessment

Shortly after the adoption of the UN General Comment No. 25 UN Committee on the Rights of the Child, General Comment No. 25 on children's rights in relation to the digital environment, the Digital Futures Commission published a report *Child Rights Impact Assessment A tool to realise children's rights in the digital environment*.[95] The report recommends that Child Rights Impact Assessments (CRIA) should be used to help entrench the best interests of the child into the digital world.[96] In the UN General Comment No. 25 itself, the Committee called for CRIAs to be conducted specifically in relation to the digital environment.[97] The report notes that CRIAs have been used in other contexts, as a mechanism for States to examine the impact of their policies on children's rights, and to ensure the visibly of children in policy-making processes.[98] It identifies that there is an important role for businesses to play in the development and design stages of products and services and notes that the education sector is one example of where children will be the end user.[99] We agree that the use of CRIAs could be a positive step forward. However, we emphasise, that there is a specific need for CRIA in the digital schooling context. We suggest that when schools are choosing which digital technologies to engage with, they mandate that only platforms which have carried out a CRIA can be used. This should include a prohibition on data processing by third parties for commercial purposes and ensure that any data that is processed is strictly related to the learning development of children. A CRIA for digital schooling would need to appropriately balance the best interests of the child and ensure that the interests of the children in receiving an education are not used a reason to allow third-party data processing to take place for unethical commercial purposes.

4.2.3 Council of Europe Guidelines on Children's Data Protection in an Education Setting

In November 2020, the Council of Europe adopted guidelines on Children's Data Protection in Education.[100] The guidelines provide principles to incorporate children's rights into digital education and make recommendations as to how law and policy makers, data controllers and the industry should do this. The guidelines integrate key rights under the UNCRC including the best interests of the child, the evolving capacities of the child, the right to be heard and the child's right to non-discrimination.

---

[94] UNICEF, 'How we Portect Children's Rights with the UN Convention of the Rihgts of the Child' <https://www.unicef.org.uk/what-we-do/un-convention-child-rights/> accessed 27 April 2021.

[95] Digital Futures Commission and the 5Rights Foundation, 'Child Rights Impact Assessment A tool to realise children's rights in the digital environment (March 2021) <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf> accessed 24 April 2021.

[96] ibid 5.

[97] UN Committee on the Rights of the Child, General Comment No. 25 on children's rights in relation to the digital environment, CRC/C/GC/25 (2021), para 23 <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t> accessed 21 April 2021.

[98] Digital Futures Commission and the 5Rights Foundation, 'Child Rights Impact Assessment A tool to realise children's rights in the digital environment (March 2021) 14-19 <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf> accessed 24 April 2021.

[99] ibid 12.

[100] Consultive Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Individuals with Regard to Automatic Processing of Personal Data, 'Children's Data Protection in an Education setting Guidelines ' Convention 108, T-PD(2019)06BISrev5, 2020 <https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b> accessed 24 April 2021.

Consistent with the UN General Comment No. 25, the guidelines state that 'Controllers and processors shall not give away children's personal data collected in the course of their education, for others to monetise, or reprocess it for the purposes of selling anonymised or de-identified data, for example to data brokers.'[101]

The below recommendation in particular would help to address the challenges of particular tensions addressed in this paper regarding whether the right to be educated and public obligations to provide children with an education are sufficient reasons to outweigh their individual data protection rights.

> To meet obligations to the rights of a child to education, settings should offer a suitable level of alternative provision of education without prejudice to the child, should families or the child exercise the right to object to data processing in digital tools, as remedy in accordance with Article 9 (1)(f) of the Convention 108+.[102]

As has been highlighted at 3.1.1 and 3.1.2, it is not clear whether a child (or parent) who exercises the right to object or withdraws their consent to using digital learning platforms will be offered an alternative. If children are not given an alternative, then they have may feel they have no choice but to agree with the way they are receiving digital education for fear that they cannot otherwise receive their learning. In line with the above recommendation of the Council of Europe, we suggest that if a child exercises their right to object, or wishes to withdraw consent, due to concerns about pervasive data collection, then they should be supported in this decision and their inclusivity should be ensured by being provided with an alternative way to learn and be included in school life. However, as is explained below, we anticipate that this could be challenging in practice due to entrenched cultural norms in schools.

5. Challenging Cultural Norms

As has been discussed, there is increasing awareness of the need to better protect children in the online world and some progress is being made in national and international regulations. However, the implementation of any new frameworks may be difficult to embed in practice. Although there has been a growing recognition of children's rights in the landscape of school education more generally, [103] there is more to be done to ensure their enforcement in the digital schooling context. This is not just recognition in the legal sense but a greater appreciation of children's rights as a digital cultural norm.

The UN General Comment No. 12 on the right of the child to be heard, a right which is protected under Article 12 of the UNCRC, stipulated that 'simply listening to the child is insufficient to be seriously considered when the child is capable of forming her or his own views'.[104] It includes the education system emphasising that this right is also fundamental to ensuring the child's right to education. Lundy has explained that 'the practice of actively involving pupils in decision making should not be portrayed as an option which is in the gift of adults but a legal imperative which is the right of the child.'[105] The UN General Comment No. 25 on Children's Rights in the Digital Environment also endorses the position that more is needed than simply listening to the voice of the child. It asserts that State parties 'should have regard for all children's rights, including their rights to seek, receive and impart

[101] ibid 7.1.12.

[102] Consultive Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Individuals with Regard to Automatic Processing of Personal Data, 'Children's Data Protection in an Education setting Guidelines ' Convention 108, T-PD(2019)06BISrev5, 2020 7.1.9 <https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b> accessed 24 April 2021.

[103] Jonathan Todres and Shani M. King, in 'Children's Rights in the Twenty-First Century Challenges and Opportunities' in Jonathan Todres and Shani M. King (ed) *The Oxford Handbook of Children's Rights Law* (Oxford University Press 2020) 722.

[104] UN Committee on the Rights of the Child, General Comment No. 12 on the right of the child to be heard, CRC/C/GC/12, 2009 para 28.

[105] Laura Lundy, 'Voice 'is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child' (2007) 33(6) British Educational Research Journal 927-942, 931.

information, to be protected from harm and to have their views given due weight'.[106] This is similar to the Council of Europe guidelines, which recommend the need for 'procedures for children to express themselves and to make their views heard in regard of exercising their right to privacy in educational settings and to ensure their view is taken into consideration'.[107] Yet the difficulty identified in this paper, that a child may not be able to exercise their right to object or the right to decline or withdraw consent in the context of digital learning platforms, is in conflict with Article 12 of the UNCRC. A mere symbolic or theoretical possibility of exercising GDPR rights does not ensure that the child's view is accorded due weight.

Byrne has argued that the extent to which children's views are given due weight is dependent, in part, upon whether the school rules are a barrier or enabler of children's rights.[108] In the digital learning context, schools, often through no direct fault of their own and often without realising, act as a barrier to children's rights. This is partially due to the lack of awareness amongst children, their parents, school staff and society at large about data protection rights, how to exercise them and why they might need to be exercised.[109] Accordingly, we are concerned as to how a child who digitally resists might be socially perceived, especially where something as important as education is at stake. Rather than being perceived as active agents of their rights, there is a risk that they might be viewed as disruptive or troublesome. The reaction is likely to be dependent on the individual school. If the above claims regarding how a child might be perceived are unfounded, a child could still hold a genuine fear as to how they will be treated socially, not only in relation to how the school will perceive them but also the reactions of peers or their own feelings of discomfort from not following the crowd. An even greater concern is that a child, or their parents, might not be aware of their data protection rights to even consider whether they would like to exercise their right to object, or to even realise that there are risks attached to data processing in the first place.

We are also concerned about the provision of alternatives. As schools will have a lawful basis for data processing, there is no guarantee that an alternative form of learning will be provided if a child or parent exercises the right to object. This makes it even less likely that this induvial right will be ultised as it adds to the concern that, by exercising data protection rights, a child's education is being compromised. It is possible that, if the right to object is exercised, some schools might respond by willingly by providing hard copies of work for instance. During the national lockdowns of the Covid-19 pandemic, some children were provided with hard copies of work and given specific time slots to pick this up from school to ensure social distancing. However, it is most likely that this provision was for children who had no or limited digital access, rather than because the right to object had been exercised. Although, this shows that an alternative to using digital learning platforms is possible, it could be logistically challenging to expect schools to do this for a more sustained period. Additionally, the fact that the provision of alternatives based on the right to object is not guaranteed, could also mean that children in one school are provided with alternatives but children in another are not.

Hierarchical structures in schools can also be a barrier to effectively respond to children's rights. Power dynamics between parents and school staff as well as systems of authority between different members

---

[106] UN Committee on the Rights of the Child, General Comment No. 25 on children's rights in relation to the digital environment, CRC/C/GC/25 (2021), para 13 <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t> accessed 21 April 2021.

[107] Consultive Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Individuals with Regard to Automatic Processing of Personal Data, 'Children's Data Protection in an Education setting Guidelines ' Convention 108, T-PD(2019)06BISrev5, 2020 6.2.3 <https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b> accessed 24 April 2021.

[108] Liam Cairns, Seamus Byrne, John M. Davis, Robert Johnson, Kristina Konstantoni, and Marlies Kustatscher, 'Children's rights to education: Where is the weight for children's views?' (2018) 26(1) The International Journal of Children's Rights 38-60, 38.

[109] Information Commissioner's Office, 'Department for Education (DfE) Data protection audit report' 5 (February 2020) <https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf> accessed 6 April 2021.

of school staff could influence how data protection issues are handled. For example, a headteacher might decide for their school to use various Google platforms. An IT manager might then be responsible for checking the feasibility of this request and a GDPR officer might only become involved if a query is raised or if the platform is one that is not widely known. Depending on the individual school culture, it could be difficult for a school GDPR officer to question the mandate of a senior colleague such as a headteacher. Their role in the school may be viewed as one that deals with data protection crises, rather than necessarily being a key part of the procurement stages when decisions are made regarding digital platforms. Further, the lack of awareness around data protection issues more generally might mean that members of school staff are not clear about when to consult the GDPR officer. How can a teacher, for example, be expected to raise an issue if they are not aware that there is a problem in the first place?

Yet, parents and school staff are important representatives for ensuring the protection of children's rights. Article 5 of the UNCRC states that children are to be guided by parents and carers in reference to the exercise of their rights, 'in a manner consistent with the evolving capacities of the child'. The UN General Comment No. 25, following consultations with children, states that children

> expressed the view that the digital environment should support, promote and protect their safe and equitable engagement: "We would like the government, technology companies and teachers to help us [to] manage untrustworthy information online."; "I would like to obtain clarity about what really happens with my data … Why collect it? How is it being collected?"; "I am … worried about my data being shared".[110]

These comments emphasise the important role of parents and teachers and that children look to those in positions of authority to support them. However, as indicated above, these individuals may be in a similarly disempowered position to children. The Council of Europe guidelines recommend that 'educational settings shall ensure that staff are trained to ensure adequate capability to understand their role in due diligence, and to be able to incorporate the right of the child to be heard.'[111] The UN General Comment No. 25 also emphasises the need for teachers to be trained on digital safeguards and help ensure that children understand the digital environment 'including its infrastructure, business practices, persuasive strategies and the uses of automated processing and personal data and surveillance, and of the possible negative effects of digitalization on societies.'[112] We agree that increased staff training is important for ensuring the realisation of Article 5 of the UNCRC in the digital education context. Better resourcing is needed to ensure that school staff have a strong awareness of data processing practices so that they have the adequate knowledge as to when to raise a data protection concern and are able to better support children in exercising rights such as the right to object.

The ultimate power imbalance is with the commercially driven third-party data processing companies and the dominant position they hold in ensuring an embedded data-intrusive culture. Their success in keeping unethical pervasive practices concealed from society at large has led to members of society, including children, parents and school staff, automatically trusting well-known platforms. Article 29 of the UNCRC indicates that education should prepare children for a responsible life in a free society. In the digital learning context, this indicates that children should be able to exercise their right to education without the coercion and disempowerment experienced, albeit unknowingly, when using digital

---

[110] UN Committee on the Rights of the Child, General Comment No. 25 on children's rights in relation to the digital environment, CRC/C/GC/25 (2021) <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t> accessed 21 April 2021.

[111] Consultive Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Individuals with Regard to Automatic Processing of Personal Data, 'Children's Data Protection in an Education setting Guidelines ' Convention 108, T-PD(2019)06BISrev5, 2020 6.2.5 <https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b> accessed 24 April 2021.

[112] UN Committee on the Rights of the Child, General Comment No. 25 on children's rights in relation to the digital environment, CRC/C/GC/25 (2021) para 105 <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t> accessed 21 April 2021.

learning technologies who engage in commercially driven data processing. Article 29 implies that there is a pedagogic imperative to stimulate a child's critical awareness around digital data protection rights. But the culture of tacit acceptance makes this difficult to address in practice.

Trust in dominant tech companies could mean that schools do not make such thorough data protection checks at the procurement stage, perhaps only undertaking detailed checks of less known apps and services. The national lockdowns as a result of the Covid 19 pandemic tipped the balance even further towards commercial companies, as many schools turned to the platforms of well-known digital technology providers, who could take advantage of the opportunity for increased data collection by affording effective pedagogic tools. The 5Rights Foundation, in their report on the Online Safety Bill, emphasised the power imbalance users face including within the education sector. They stated that,

> In bringing forward an Online Safety Bill, the government has recognised that individual users — particularly children and parents — are in an asymmetric power imbalance with the demands and commercial interests of tech companies. By exempting EdTech, the government has failed to extend this acknowledgement to teachers who cannot and should not be expected to mitigate the negative impacts of the digital services on which schools and children rely.[113]

This important observation makes clear that more input is needed to address the power imbalance in the education sector. School staff should be supported in protecting and empowering children and adequate resourcing is needed to ensure this. However, school staff should not be entirely responsible as the Government and technology companies themselves also have a role to play.

6. Key Recommendations and Conclusions

Children spend vast amounts of time engaging with the digital world. This increased during the Covid-19 pandemic when national lockdowns meant that most children had to undertake their schooling remotely. The collection of 'learner data' through digital learning platforms exposes children to unethical data processing by third-party companies, who use the data for commercial gain. Technology companies have strategically increased their product marketing during the Covid 19 pandemic, including through providing free or low-cost services. This has given companies increased influence over the education sector and helped to cement data-intrusive norms in the schooling environment. The speed at which schools had to transition to online learning left little room for full consultation on which digital platforms would be used.

The UK GDPR outlines individual data protection rights to safeguard personal data and special category data. The vast majority of data collected via a digital learning platform is personal data, for which children or their parents can exercise the right to object under Article 21. However, the practical reality of exercising this right in the schooling context is fraught with difficulty. Schools can legitimately rely on 'public task' and 'legitimate interest' justifications in Article 6(1)(e) and (f) of the UK GDPR as the school has a legal duty to educate and children have a right to be educated. Any special category data processed for digital learning can also be processed lawfully where there is 'substantial public interest' as per Article 9(2)(g). The commercial use of anonymous 'learner data' is also not entirely risk-free.

Although the UK GDPR constitutes a commendable political effort to legally regulate and enforce how companies process data on individuals, the legal framework leads to friction for both the school and the child learner, which current DfE guidelines do not clarify. Fundamental to the problem is the fact that schools are generally UK GDPR compliant. It is the legal framework itself that leaves a gap for third party companies to creep into. The right to be educated and the public obligation to provide an education are clearly entrenched in law but we suggest that these are not good enough reasons to warrant exposing children to exploitative data processing practices which are likely to have a negative impact on their

[113] 5Rights Foundation, 'Ambitions for the Online Safety Bill' (April 2020) 9 <https://5rightsfoundation.com/uploads/Ambitions_for_the_Online_Safety_Bill.pdf> accessed 23 April 2021.

future. Schools have little guidance as to how to balance the individual rights of the child with the wider their public duty and it is not clear whether there is a uniformed approach.

The cultural dynamics of the digital learning environment are also a barrier to the realisation of children's rights and can make it difficult for a child, or their parent, to exercise data protection rights. The socially disempowered position of children in the digital learning context is related to several issues including social fears regarding how a child who objects might be perceived and hierarchical structures in schools between children and school staff as well as systems of authority between staff themselves. The provision of alternatives for children is not guaranteed and creates logistical issues for schools. Most concerning is the power imbalance experienced by children, and those who are responsible for protecting them, as a result of the commercially driven data-intrusive norm which technology companies have taken even more advantage of since the Covid 19 pandemic. It is hoped that developments in national and international instruments might go some way addressing this imbalance but, as has been demonstrated, much of the existing and proposed regulations take a broad view, rather than specifically considering 'learner data'.

We recommend the following in order to afford better protection to 'learner data':

- Clarification of the risk-benefit balance of digital technologies in the schooling context, including more detailed guidance for schools as to how to balance educational rights and responsibilities with individual data protection rights.
- Practical support for schools as to how to handle a situation where a child or parent exercises the right to object.
- Greater consideration by relevant stakeholders as to how a child's right to object can be made more socially acceptable.
- A guarantee of alternative provisions made to children who exercise the right to object.
- A national unified response as to how schools can provide a high-quality education, and utilise the pedagogic benefit of digital learning technologies, without exposing children to the risk third-party data processing for commercial purposes.
- National consideration of how digital learning tools can be funded so that schools are not compelled to consider only free or low-cost options, which are more likely to operate on surveillance capitalism.
- Recharacterise the EdTech sector through consideration of whether some economic benefit can be sustained, while also addressing the social, legal, ethical, and practical challenges with greater care and attention.
- Government regulation which specifically addresses the digital schooling environment.
- Mandatory Child Rights Impact Assessments for digital learning tools.
- Explicit UK commitment to the UN General Comment No. 25 on children's rights in relation to the digital environment, including how it will be reflected in school education.

This paper ends with a final message of global relevance. Societies need to reflect on whether they are satisfied with an education system that allows children to be exploited for commercial gain. Following the implementation of the UN General Comment No. 25, now is the time to consider whether we wish to remain in the disempowered position in which we live and allow the invisible data-intrusive culture that commercial companies have carefully crafted to prevail. Public exposure as to what exactly is happening to our children's 'learner data' is vital.

Education in a Datafied World: Balancing Children's Rights and School's Responsibilities in the age of Covid 19

Emma Nottingham, Caroline Stockman, Maria Burke

University of Winchester

Sparkford Road,

Winchester

SO22 4NR

Corresponding author: Emma.Nottingham@winchester.ac.uk

Author Bios

Dr Emma Nottingham is a Senior Lecturer in Law, and Fellow of the Higher Education Academy. She is the Co-director of the Centre for Information Rights at the University of Winchester, UK. Her research focuses on the intersection of social, legal and ethical rights of children in various contexts including the digital world, broadcast media exposure and healthcare.

Dr Caroline Stockman is a Senior Lecturer in Education Studies, and Senior Fellow of the Higher Education Academy, at the University of Winchester, UK. Her research centres on the human-technology relationship, with a cultural-political focus. She also draws on professional experience working within the commercial e-learning industry. Her doctoral study considered technology acceptance in education.

Professor Maria Burke is a Professor of Management in the Department of Responsible Management, University of Winchester, UK. Her research concerns the area of information management and digital systems, both present developments as well as with a view on future society, and specifically in relation to business ethics.

Acknowledgements

This research was funded by Human Data Interaction- A UK EPSRC Network Plus.

Thank you to Christine Rinik for comments on earlier drafts.