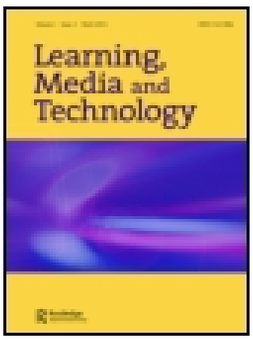

Learning, Media and Technology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cjem20

Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech

Emma Day, Kruakae Pothong, Ayça Atabey & Sonia Livingstone

To cite this article: Emma Day, Kruakae Pothong, Ayça Atabey & Sonia Livingstone (2022): Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech, Learning, Media and Technology, DOI: 10.1080/17439884.2022.2152838

To link to this article: https://doi.org/10.1080/17439884.2022.2152838

Published online: 20 Dec 2022.

LEARNING, MEDIA AND TECHNOLOGY
https://doi.org/10.1080/17439884.2022.2152838

Routledge
Taylor & Francis Group

RESEARCH ARTICLE

OPEN ACCESS Check for updates

Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech

Emma Day [a], Kruakae Pothong [c], Ayça Atabey [b] and Sonia Livingstone [c]

[a]Tech Legality OU, Tallinn, Estonia; [b]Law School, University of Edinburgh, Edinburgh, UK; [c]Department of Media and Communications, London School of Economics and Political Science, London, UK

ABSTRACT

A socio-legal analysis of the UK governance regime for data collected from children at school for teaching and learning contrasts the government-mandated data collection by schools to inform educational policy and planning with data processed and shared with third parties by commercial EdTech providers. We find the former is effectively governed by the government's 'Five Safes Framework' with some problematic exceptions. By contrast, EdTech providers process a growing volume of personal data under the DPA 2018/UK GDPR with a looser enforcement regime. While schools have few mechanisms and insufficient expertise or resources to hold EdTech providers accountable for processing children's data, EdTech providers have considerable latitude in interpreting the law. Consequently, and paradoxically, regulations governing (mostly) deidentified data used for public purposes are more systematically enforced than those governing personal (identifiable) data used for public and commercial purposes. We conclude with recommendations so that education data can serve children's best interests.

ARTICLE HISTORY
Received 21 February 2022
Accepted 21 November 2022

KEYWORDS
Education data; data protection; EdTech; child rights; governance regime

Introduction

Society is becoming reliant on education technology (EdTech) for its provision of education at all levels and to advance government and commercial interests in education-related data sharing. Uses of technology increasingly underpin children's learning in ways that transform curricula, pedagogy and assessment as well as the management and social experience of school. Accelerated by the COVID-19 pandemic, the growth in EdTech creates opportunities for data from and about children to be processed for many educational, commercial and other purposes within and beyond the school, some but not all in the public interest. The resulting 'datafication' of education (Bradbury 2019; Williamson and Hogan 2020; Selwyn, Pangrazio, and Cumbo 2021; Peters 2022) and childhood (Barassi 2020; Mascheroni and Siibak 2021) raises pressing questions about the governance of data collected through schools and the benefits and harms that may ensue. This article critically examines UK law and policy to determine whether the government, as the overall duty bearer for children's privacy and data protection rights, maintains oversight and control.

Researchers from many fields, including education, sociology, information and technology studies and psychology, are uncovering a host of emerging data-driven practices in schools. These relate to the uses of school information management systems, learning analytics, artificial intelligence (AI), personalised learning, quantified disciplinary practices, surveillance-based

CONTACT Emma Day dayemm@gmail.com

systems of safeguarding, and more. However, the governance regime that applies to personal data in educational contexts is not well understood. Although good governance and the rule of law require primary legislation to be laid down by Parliament and to be subject to debate, the UK government has not produced legislation specifically concerning EdTech or education data. We undertake a socio-legal analysis to assess whether and how the UK's data governance regime enables schools to achieve their educational purposes while protecting the interests of children and the wider public.

Why the processing of children's education data matters?

Data are appreciating in value, resulting in market pressure for data to be collected, processed, shared and reused more fluidly, as reflected in the UK's data priorities (DCMS 2021). In education, data have always been processed from children in schools, for some data processing is necessary for the school's functioning and to monitor the educational development of individual children. But increasingly, such data processed from children in schools are facilitated by EdTech, an already major and expanding sector with a projected value of £3.4bn in 2021 (IBIS Capital 2019). The growth of EdTech use in schools is promoted by the Department for Education's (DfE) EdTech Strategy, which sets out a vision for EdTech to be an 'inseparable thread woven throughout the processes of teaching and learning' (DfE 2019, 4) even before the need for remote education during Covid 19 lockdown (DfE 2021a). Yet the Strategy gives little weight to data protection beyond noting the importance of preventing data breaches and pointing to DfE's Toolkit, a non-binding guidance document that offers 'Guidance and support for education providers who want to increase their use of EdTech' (DfE 2018a).

The scale of education data processing by EdTech companies increased significantly since the COVID-19 pandemic forced UK schools online for extended periods. Already exceeding DfE's projection, the UK EdTech sector grew 72% by November 2020, bringing its value to almost £3.5bn (Walters 2021). The pandemic prompted the UK government to spend £60 m on a contract with Computacenter (UK) Ltd to supply 'laptops and tablets' including 'Google and Microsoft Educational Operating System Licences to use any Deliverables supplied by the supplier' (DfE 2020). In May 2021, the Minister for the Cabinet Office acting through Crown Commercial Service (2021) established an agreement for Cloud services worth £750 m to be supplied by ten suppliers, including Google Commerce Ltd. Google reported in May 2021 that their global user numbers for Google Classroom rose to 150 m from 40 m the previous year (Williamson 2021). Yet, in the rush to provide education to children worldwide during COVID-19 lockdowns, little critical attention appears to have been paid by the government to the data protection implications of the EdTech tools deployed.

The main value of data lies in the insights and predictions that result from data analysis. This can inform evidence-based policy by enabling education authorities to track aggregate student progress across diverse settings and identify the external factors that make a difference to target resources and plan interventions (Livingstone, Pothong, and Atabey 2021). It can also drive innovation in and uptake of EdTech that may improve educational outcomes for children by facilitating formal and informal communication and learning within and beyond the school (Lynch, Singal, and Francis 2021; Stringer, Lewin, and Coleman 2019), promoting the personalisation of teaching and learning (Komljenovic 2021; DiCerbo 2016), and creating opportunities to observe an individual child's progress in comparison to others or deploy assistive technologies to support children with physical or learning disabilities (Lindeblad et al. 2017; Lynch, Singal, and Francis 2021; UNICEF 2021). Learning analytics automated through algorithms or applications of AI are increasingly used in teaching (Kurni and Srinivasa 2021; Luckin and Çukurova 2019), administrative decision-making and resource allocation (Siemens and Long 2011; Williamson and Piattoeva 2019; Macfadyen and Dawson 2012), in information management processes, and to meet growing requirements of school safeguarding (DCMS 2020).

Although the routine use of EdTech in the classroom is widely taken for granted by schools and families (Livingstone and Sefton-Green 2016), the promised benefits are not reliably realised. The Education Endowment Foundation's evidence review by Stringer, Lewin, and Coleman (2019, 25) finds 'evidence that the use of technology to enhance learning can be positive across a range of subjects. Gains are often small, resulting on average in around two to three months' accelerated learning for children who use technology'. Noting 'huge variability in the evidence' (33), it concludes cautiously that '[e]vidence suggests that supplementing standard teaching rather than replacing it with technology interventions can have the most positive impact' (32). Meanwhile, critical concerns are growing. The debacle over the algorithm developed by the Office of Qualifications and Examinations Regulation (Ofqual) to predict national exam results by postcode in the summer of 2020 (Coughlan 2020) was, arguably, EdTech's equivalent of the Cambridge Analytica scandal. In the public mind, this suggested abuse of education data resulting in unfair grading that adversely affected students' educational progression (Smith 2020). Not only is there much that can go wrong in sharing data – witness also the National Cyber Security Centre (2021) report of an increase in ransomware attacks on schools – but there are critical questions to be asked about whose interests are served by the current policy.

Notwithstanding that some EdTech products and services are provided 'for free,' the huge economic value extracted by EdTech through third party sharing and mining of education data in the wider data ecology arguably goes beyond any 'quid pro quo' and is potentially or actually exploitative (Williamson and Hogan 2020; Persson 2020). Not only do companies profit from access to children's personal data gained in real time throughout the school day, but they may be shaping what children are taught and how (Gulson et al. 2021). In short, any risk-benefit analysis of children's data processed by EdTech remains contested on pedagogic, economic, inclusion and/or data protection and privacy grounds (Veale 2022; Witzenberger and Gulson 2021; Selwyn 2015; Macgilchrist 2019; Persson 2020; Williamson and Piattoeva 2019). Furthermore, while children's data is shared via their schools to EdTech companies, EdTech companies do not return the data to schools in a usable format to improve education unless sold as a data analytics product (Persson 2020).

Definitions and methods

Personal data is information that, on its own or in combination with other information, can identify 'natural persons' (ICO 2021b, 10). Processing personal data is regulated under the Data Protection Act (DPA) 2018 and UK General Data Protection Regulation (UK GDPR). The DPA 2018 defines 'education data' as 'personal data which consists of information that forms part of an educational record; and is not data concerning health.' In practice, this 'includes most information about current and past pupils that is processed by or on behalf of a school' (ICO 2020c, 67). Thus, 'education data' encompasses not only data collected for teaching, learning and assessment but also that used for safeguarding and administration. Moreover, the same data can serve educational and non-educational purposes. For instance, attendance records appear administrative but are used as a proxy for both educational outcomes and safeguarding. This complexity is exacerbated by the move to 'all-in-one' or whole-school products such as Google Classroom or Microsoft Education during the pandemic. Consequently, rather than comparing the regulation of particular kinds of data or data processing purposes, we compare the two main governance regimes that apply to children's data processed by or on behalf of schools for purposes of learning and assessment.

The first concerns the termly school census, which mandates state schools under the Education Act 1996 to collect certain data for public purposes such as the planning, budgets, and policy development of local and national government. The second concerns all the personal data collected from children during their school day and processed by EdTech providers who have contracted with UK schools. Both are regulated by the data protection legal framework in the UK (DPA 2018/UK GDPR). The census data form part of DfE's National Pupil Database (NPD) which, in turn, can

be linked to other official datasets. Access to these falls under the Digital Economy Act's (DEA) 2017 'Five Safes' regime for publicly held data. No additional regime applies to data processed by companies, although the recently introduced Age-Appropriate Design Code (AADC) (ICO 2020a) offers children some additional protections when EdTech tools are classed in law as information society services, which is not always the case in schools.

This article asks how the data processed from children in educational contexts are governed and whether this is in children's best interests. We focus on UK state schools (formally, 'state funded schools') because they are public authorities subject to enhanced government oversight, including certain obligations prescribed by the UK GDPR (such as appointing a data protection officer (DPO) and responding to students' data subject requests under the Freedom of Information Act 2000) from which private schools are exempt. Our methods were threefold. First, we drew on desk research on laws, policies, government strategy papers, private sector policy papers and grey literature related to data governance and children. Second, we conducted 36 expert interviews about data governance in UK schools with school governors, head teachers, school DPOs, commercial DPO service providers, relevant NGOs, education union staff and academics. Third, we held an expert roundtable with 26 stakeholders (Livingstone, Pothong, and Atabey 2021) to deliberate the benefits and harms of processing education data and any need for improved governance.

Two governance regimes for data collected from children at school

The five safes framework

Schools collect termly census data, which feeds into the DfE's NPD. In processing children's data pursuant to Section 537 of the Education Act 1996, schools are required to comply with the DPA 2018, the UK GDPR, the Human Rights Act (HRA) 1998 and the Equality Act (EA) 2010. The NPD includes the child's name and address, UPN (the Unique Pupil Number assigned to children by local authorities on their first entry to state schools), ULN (the Unique Learner Number for those aged 14+), date of birth, gender, ethnicity, language, special educational needs and disability, eligibility for free school meals and pupil premium, engagement with social services, school attendance, suspensions and exclusions, and more (DfE 2022b). It is likely that parents and children know that they have provided these data to the school and, though they may not realise what is shared with the government nor how it is used, they expect this to serve legitimate public purposes (Stoilova, Livingstone, and Nandagiri 2020).

As a public body, the DfE is required to comply with the DEA 2017 (Chapter 5) and its accompanying statutory code, which restricts the sharing of publicly held data for research purposes only to deidentified data. It declared its adherence to the Five Safes Framework (ONS 2020) from around 2018, presumably to demonstrate compliance with the DEA 2017. Developed in 2003 by the UK Office for National Statistics (ONS) to 'address … data access solutions' for 'confidential research data at ONS' (Desai, Ritchie, and Welpton 2016, 5), this framework is still in use as a mechanism to 'protect data confidentiality' (ONS 2021, 10) as it provides access to the deidentified survey and administrative data for statistical research and supports an evidence base for public policy decision-making, public service delivery and academic research (Silberman 2021; Groos and van Veen 2020; Ritchie 2017, 2–3). It has been adopted by other statistical agencies, data archives and government departments in the UK and abroad (Ritchie 2017, 1).

To access the NPD, applicants must be accredited under ONS approved researcher scheme and document in their application to the DfE how they ensure 'safe people' (by, for instance, a criminal record check), 'safe projects' to prevent security breaches (Landau 2018), 'safe settings' (data access is only possible using ONS secure technology systems), 'safe outputs' (that do not identify data subjects), and 'safe data' (deidentified data). Applications for NPD data shares are mostly processed by the Data Sharing Approval Panel (DSAP) which determines 'what data is available and the best way to access it', whether through the ONS or secure file transfer directly from the DfE on the condition

that the company's IT and building security is sufficient and that the company does not keep the data for longer than allowed (DfE 2022a; ICO 2020b). In practice (according to the DfE's own records of data shares), the secure file transfer from DfE is inconsistent with the Five Safes Framework, particularly the 'safe settings' and 'safe data' that are strictly adhered to in data access through ONS, as demonstrated later.

DPA 2018/UK GDPR

EdTech used in school for teaching and learning includes organisational platforms by which teachers manage children's timetables, homework and home-school communication, classroom tools (including digital workbooks and specific curriculum apps). Some of these monitor engagement, offer personalisation, or deploy tools that use algorithms to predict grades or other outcomes. Diverse kinds of data are collected at multiple time points, including metadata passively taken from children (e.g., IP address, device information, unique device identifiers, mobile network information and phone number) (Persson 2020) or inferred about them through automated processing such as profiling (Selwyn 2015). Children and their parents have little choice but to sign schools' 'Acceptable Use' policies although they may not understand the seamless processing of their data by EdTech and other companies, nor how to exercise their data subject rights under the UK GDPR (Chapter 3).

Education data processed by EdTech companies through their contracts with schools are primarily regulated through the DPA 2018, which sits alongside and supplements the UK GDPR. The UK GDPR sets out seven core data protection principles 'which lie at the heart of the general data protection regime' (ICO 2021b, 17) and underpin the individual rights of data subjects (Gil González and De Hert 2019; European Data Protection Board 2020, 9). If we read Article 5(1), which sets out the first six principles, with schools and EdTech providers in mind, this requires (a) *lawfulness, fairness and transparency* (where 'lawful' requires schools and EdTech providers to rely on the lawful bases in Article 6 and ensure that their processing is legitimate; 'transparency' requires being clear, open and honest about data processing; and 'fairness' requires only processing data in ways that children would reasonably expect and not use it in ways that would negatively affect them (ICO 2021b, 21)); (b) *purpose limitation:* (schools and EdTech providers must be transparent about their data processing purposes and undertake these only for the original purposes they communicated to data subjects); (c) *data minimisation:* schools and EdTech providers must ensure that data processing is adequate, relevant and limited to what is necessary for the purposes; (d) *accuracy:* schools and EdTech providers must ensure that the data they process is accurate and, where necessary, up to date, and they must take reasonable steps to erase or rectify personal data that are inaccurate; (e) *storage limitation:* schools and EdTech providers can only store the data for the period necessary for the defined purposes, and must be able to justify this period; (f) *security:* schools and EdTech providers must take appropriate security measures to protect the data processed.

Article 5(2) UK GDPR introduces the seventh principle of accountability which requires data controllers (including schools and EdTech providers that act as data controllers) to be able to demonstrate compliance with Article 5(1) principles. Aligned with Article 5(2), one of the accountability obligations provided under Article 25 (data protection by design and by default) requires controllers to embed Article 5 principles into the design of processing operations and ensure the highest privacy protection (ICO 2021b). Building on Article 5(1)(a) and Recital 38, the Information Commissioner's Office (ICO) (2020a, 12-25) introduced the AADC as a statutory code of practice following a requirement under Section 123 of the DPA 2018 to provide guidance 'on standards of age-appropriate design of relevant information society services (ISS) which are likely to be accessed by children.' In effect, this sets out children's rights in relation to UK data protection law.

Governance regimes compared

Neither governance regime is specific to education, possibly explaining why the DfE has provided no guidance for processing education data. Nor does either say much that is specific to children, though both regimes recognise children as vulnerable data subjects who require stronger protections. However, these regimes were developed with different aims and objectives, so although they can apply to the same data, they differ in how they protect the rights of children as data subjects (see Table 1).

The Five Safes Framework was designed to manage the risks of identification to individuals by taking steps to deidentify data subjects, ensure the security of the data and control access to their data. It centres on the data user rather than the data subject, and 'data access planning starts with the identification of user needs' (Ritchie 2017, 2). By contrast, the DPA 2018/UK GDPR is premised on the idea that personal data identifies an individual, and its aim is to protect the rights of the data subject throughout the data ecology. While the Five Safes Framework balances risk to the data subject with the public benefit that can accrue from data sharing, the DPA 2018/UK GDPR seeks to balance the rights of data subjects with a broad range of interests in data sharing and usage (Lynskey 2015), including by commercial organisations. This effort to balance competing interests in the value of data – whether focused on the public or private sector – generates problems for children's rights, as we explore next.

Problems with the governance of access to the national pupil database

Since the NPD holds personally identifiable data, processing of such data for other than law enforcement purposes must comply with both the Five Safes Framework, meaning that deidentified data cannot be reidentified nor can identifiable data be taken from the 'safe setting,' and the DPA 2018/UK GDPR. However, the latter did not come into force until 2018 while the DfE's external data sharing practices had been established from 2002. Our expert interviews reported an increase in demand from a broad range of organisations following the then Secretary of State for Education Michael Gove's decision to 'enable the Department for Education to share extracts of data held in the NPD for a wider range of purposes than currently possible in order to maximise the value of this rich dataset' (Gove 2012). This decision resulted in an amendment to the 2009 Prescribed Persons Act in 2013 to allow the DfE to share both deidentified and personally identifiable pupil level data in the NPD with external parties beyond academic researchers. The DfE (2017) recorded 481 external data shares (inclusive of duplicates) from July 2012 and September 2017. These included 82 external data shares with commercial entities, of which 75 were of the NPD; the rest were marked as 'linked' data. Companies such as ALPs (later known as Alkemygold Ltd) and Fischer Family Trust (FFT) were granted access to either 'identifiable and highly sensitive' or 'identifiable and sensitive' data in the NPD to develop analytics tools to improve school performance (DfE 2017).

Table 1. Two governance regimes for education data

Five Safes Framework	DPA 2018/UK GDPR
Aim: To control who can access and process personal data held by the government	**Aim**: To protect the rights of data subjects when their data are processed
Approach: Risk-based and user-centred (Arbuckle and Ritchie 2019; Ritchie 2017, 2)	**Approach**: Risk- (Gellert 2016) and rights-based (Lievens and Milkaite 2018; van der Hof 2018)
Objective: To implement a control mechanism that ensures an 'ethical/legal/logistical basis for access' to data (Ritchie 2017, 2)	**Objective**: To balance 'free trade in personal data in the EU internal market' with the 'protection of fundamental rights' (Lynskey 2015, 8)
Beneficiaries: Researchers, research institutions, policy makers, public bodies, R&D branch of commercial entities	**Beneficiaries:** Data subjects and data users

The range of external parties with whom the DfE can share pupil level data was meant to be tightened up by the DEA 2017 and the DfE's declaration of its adherence to the Five Safes Framework. However, our analysis of the six DfE external data share records published bi-annually from May 2018 to June 2021 shows that sharing high-risk (of identification or reidentification) data with commercial entities continues. In combining these six records, we included data from the 'DSAP considered data shares' tab and eliminated the duplicates, resulting in a total of 467 external data shares. Of these, 117 (25%) were shared with 40 unique commercial entities – most offering consultancy services (16), data analytics (5) or software services (5); 84 (72%) shares were of the NPD. The rest were of Individualised Learner Records (ILR) or other data held by the DfE, such as the School Workforce Census. The purposes of data access stated by the approved 117 commercial companies ranged from statistical analysis and providing evidence to support 'government decisions about investment in vocational education and training' to setting standards for GCSE qualifications, as well as to 'improve GCSE mathematics retake outcomes,' undertake 'randomised controlled trials of educational programmes' and 'develop' commercial analytics tools.

The proportion of the NPD shares with commercial entities is a minority of the whole, and the purposes are arguably in the public interest. Still, there are grounds for concern. Only (deidentified) 'safe data' is meant to be shared by DSAP, but of the 84 NPD shares with commercial entities, 18 (23%) shares included either Level 1 'instant identifier' (e.g., full names, addresses, email addresses) or Level 2 'meaningful identifiers' (e.g., UPN, ULN, or national candidate numbers) (DfE 2021b). In principle, these could be combined with other data, increasing the risk of identification. Further, from the 18 shares of Level 1 and Level 2, 16 (84%) were shared through 'secure file transfer directly to the organisation.' Ten of these were for projects commissioned by the DfE, government agencies or universities, and four contained 'highly sensitive data about interactions with children's services' (DfE 2021c).

To give an example, King's College London commissioned a consultancy company, Kantar (Case number DS00513), to recruit participants for a longitudinal survey to examine the 'differences in attitudes and knowledge between sub-groups … to help shape priorities in post-16 education and training' (DfE 2021c). To enable this, Kantar was granted access to NPD data that contained Level 1 'instant identifiers' through 'secure file transfer directly to the organisation'. Another example is DfE's share of Level 1 ('instant identifiers') NPD data with FFT Education Ltd (Case number DS00120) through 'secure file transfer directly to the organisation' in response to the company's application 'to develop and deliver analyses that are of benefit to … schools, local authorities, academy chains and diocese through a web based analytical service called "FFT Aspire"' (DfE 2021c), itself a commercial service offering 'comprehensive online reporting and data analysis' for educational bodies (FFT Education Ltd 2020).

These examples of high-risk data shares delegate control and responsibility over how data are protected, secured and processed to the recipient organisations. The secure transfer of Level 1 and Level 2 data directly to such organisations is inconsistent with the original intent of the ONS Five Safes Framework (UK Data Service 2022) under which researchers can only access (mostly) de-identified data in an environment physically controlled by the data owner to protect against confidentiality breaches and unauthorised use. Our analysis finds these high-risk data shares to be more common with commercial (mostly consultancy or data analytics) companies (14 shares) than with academic institutions (3 shares), for as one expert interviewee observed, academic researchers rarely ask for instantly identifiable data. The question arises as to whether the safety and security risks of personally identifiable data sitting in the computing and storage devices of universities, companies and other organisations are proportionate to the benefits of the secure file transfer. It is also unclear whether audits are ever conducted to ensure that data are only kept for the time period agreed.

Indeed, the DfE's external data shares with commercial entities can beproblematic. In November 2022, the ICO reprimanded the DfE for failing to comply with the UK GDPR (Article 5(1)(a) to guard against "the unauthorised processing by third parties of data held on [DfE's Learning Records

Service (LRS)] database"] and failing to comply with the UK GDPR (Article 5(1)(f) to protect the confidentiality of data subjects (ICO 2022). This incident allowed third-party betting companies to use personal and special category data in the database for age-verification checks (Ungoed-Thomas, 2022). Previously, in its *Data Protection Audit Report*, the ICO (2020b, 6) found that '[w]hilst DSAP is the official gateway for shares, not all sharing decisions throughout the DfE and its executives agencies are considered by DSAP, so there is limited oversight and consistency around how data is shared externally.' It also found a lack of assessment of applications for their data protection compliance because DSAP does not formally or consistently assess applications for this purpose, and nor does it require applicants to conduct a data protection impact assessment (DPIA) (ICO 2020b, 6). Finally, the ICO (2020b, 6) criticised the DfE for its 'over reliance on using public task as the lawful basis for sharing which is not always appropriate and supported by identified legislation'. In summary, while the Five Safes Framework is robust when used as originally intended, DfE practice over the years has introduced risks of identification, reidentification or reuse and is not fully consistent with the DPA 2018/UK GDPR.

Problems with the governance of EdTech data processing

The only way to access children's education data at a national level used to be through a data access application to the DfE's DSAP, which had to meet the standards of the Five Safes Framework. Schools' expanding use of EdTech tools has facilitated EdTech providers' access to data about children on a significant scale. Governed by the DPA 2018/UK GDPR but with very little oversight, this data processing raises several problems.

The first lies in establishing the scope of liability between contractual parties – schools and EdTech providers. Under the UK GDPR (Article 4(7)), the data controller is responsible for deciding which data are processed, how, and for what purposes, while the data processor undertakes the processing activity accordingly (Article 4(8)). Both are accountable for data processing, but the controller's liability is greater. Even though most EdTech companies position themselves as data processors, their processing activities show that they act as data controllers. For example, in 2020 Google was found to use the data it collects via Google Education for its own commercial purposes (United States District Court for the District of New Mexico 2020, 14), contrary to its role as a processor. Identifying the data controller is a matter of fact, not self-declaration and should be based on an assessment of actual control over the data processing. Yet our interviews revealed complexities because, although schools are deemed (by the ICO, by some EdTech providers) to be data controllers, they may lack the expertise and resources to ascertain the purposes, nature and extent of the data processing. Indeed, the operation of EdTech services can be obscure even for lawyers (Nas and Terra 2021). Also problematic is when schools are deemed joint data controllers with the providers of the EdTech, a situation which leads to complicated liability issues and unclear accountability.

A second problem concerns the lawful basis for processing personal data, which can be at odds with the data subject's 'right to object' in schooling contexts (Nottingham, Stockman, and Burke 2022). Where schools are controllers, the lawful basis for processing is usually 'public task' (Article 6(1)(e) UK GDPR). However, the public task of education is not clearly defined, leaving schools to determine not only the legal and technical but also the pedagogical parameters for proportionate and necessary data processing in procuring and enforcing contracts with EdTech companies.

Both these problems are exacerbated by the growing use of AI. As data controllers, schools must uphold child data subjects' rights 'not to be subject to a decision based solely on automated processing, including profiling' (Article 22 UK GDPR), but in the absence of explainable AI (Samek and Müller 2019), this is challenging (5Rights Foundation 2022). Indeed, especially when dealing with major companies whose operations are far from transparent (5Rights Foundation 2021), hard-pressed schools often face little choice in practice but to trust the assurances they receive from EdTech and agree on a contract. Illustrating this reality, we learned that although the UK GDPR requires a DPIA for processing children's personal data for purposes such as profiling children

or offering online services directly to them, schools often rely on wording for the DPIA drafted by the EdTech providers themselves (Livingstone, Pothong, and Atabey 2021).

Third, a crucial complication arises when an EdTech provider offers optional features over and above those required for its core educational purposes, for then it becomes an independent data controller for non-core purposes. An example is the use of Google Maps alongside Google Classroom in a geography class. In such cases, which are commonplace, children's data cannot be processed on the lawful basis of public task. This problem is far from accidental, for it is likely to be part of Google's business model to provide a service as a data processor to schools in such a way as to promote its own additional (non-core) services (Hooper, Livingstone, and Pothong 2022). EdTech providers may use the 'legitimate interests' lawful basis for purposes such as marketing or product development when the processing is 'necessary' and when there is a balance between the interests of the EdTech providers and the best interests of child data subjects. However, this balancing task is complex, and it brings additional responsibilities under UK GDPR to respect data subject rights. Currently, there is very little oversight by the government regarding how this is achieved in practice.

Meeting the specific needs of children as data subjects improved when the UK's AADC came into force in 2021. But whether and how this applies to EdTech companies or schools is mired in confusion – our fourth problem. Our expert interviews surfaced conflicting answers, as we and others have communicated to the ICO. In the summer of 2021, the ICO (2021a) responded by clarifying that the AADC applies to off-the-shelf EdTech services 'provided to children through a school' but not when the EdTech service is offered 'via an intermediary such as a school' to 'fulfil the school's public tasks' and acting 'solely on the instruction of the school'. As may be imagined, this has not resolved the confusion.

Of importance is that the AADC applies only to ISS, defined in Article 1(1) Directive (EU)2015/153 (European Parliament 2015) as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services', which are offered directly to a child (ICO 2021c). The criteria of provision at a distance, by electronic means and normally for remuneration, are not in dispute: all apply to EdTech. What matters is that if EdTech is offered through a state-funded intermediary such as a school to 'fulfil the school's public tasks' (ICO 2021c), then EdTech in this context *may not be* a 'service' under Article 50 of the Treaty establishing the European Community (European Union 1957) because it is seen as an online extension of the school's public task (here, education), and therefore not an ISS.

We argue that most EdTech services used by schools to deliver remote learning and connect teachers with children and their parents (e.g., Google Classroom and Class Dojo) satisfy all the conditions of ISS as students must individually request the last-mile transmission of the service to their individual device for their own use. We also argue that EdTech is a commercial 'service' procured by schools for children to use just as schools procure chairs for children to sit on, which does not make the supplier of the chairs a provider of public service. The same typically applies to 'off-the-shelf' apps used in class when students individually log in and/or interact with the apps.

Yet other EdTech services, such as the management information systems (MIS) offered by Capita Group or software used for administrative tasks or improving schools' performance, are not ISS because although they process children's data, children do not individually request this. Note, however, that even if the AADC does not apply, since it merely prescribes how the UK GDPR protects children, its standards are still relevant to all organisations processing children's data (ICO 2020a, 11), and it would be unfortunate if EdTech companies chose to use a lower standard for children on the basis of a technicality.

The fifth and most compelling problem concerns the insufficient implementation of the DPA 2018/UK GDPR by the UK government in the form of binding standards and guidance for schools on the use of EdTech. Despite encouraging EdTech uptake in UK schools and highlighting its benefits for teaching and learning (DfE 2019, 32), the DfE has not provided a legally binding EdTech procurement framework or recommended contractual terms, nor endorsed particular EdTech services or provided assessment tools for schools to evaluate EdTech services on the market

(Day 2021). We argue that this is a clear task for the government and is wholly unfair (to both schools and children) to require schools to negotiate the terms and conditions of contracts with EdTech companies – which include multinational tech giants – on a school-by-school basis.

Given the above problems, it is unsurprising that the ICO's (2019) consensual audit of the 11 MATs between 2018 and 2019 reveals schools' poor compliance with data protection laws. Note that the ICO has the power to conduct compulsory audits under Article 58(1)(b) UK GDPR but has yet to exercise that power on EdTech providers or schools as it has with the DfE. This leaves schools without official feedback or guidance (Turner, Pothong, and Livingstone 2022), impeding their capacity fully to consider data protection when procuring EdTech services or seeking to hold EdTech providers accountable to schools and children.

Two governance regimes for data collected from children at school

This article has identified problems with the implementation of both the data governance regimes that regulate access to children's data collected at or through school. However, by comparison with the Five Safes Framework's regulation of access to data by public bodies, the enforcement of the DPA 2018/UK GDPR regime concerned with data processing and sharing by the private sector raises far bigger concerns. These arise from uncertainties or inconsistencies in the interpretation and application of data protection laws, exacerbated by the complexity of the relationship between EdTech providers and schools and the absence of concerted sector-specific audit and enforcement by the DfE and ICO. As a result, schools face the formidable burden of navigating a complex and fragmented legal and technical landscape concerning the data processing that has become part and parcel of their work. Not only do schools lack expertise and resources, as well as straightforward enforceable guidance from the government, but there is a considerable power imbalance between schools and EdTech providers. This avails EdTech providers instant access to data collected from children in schools with insufficient oversight, transparency or accountability and with considerable latitude to interpret and apply the law as they choose, including making the required proportionality assessment about the balance between children's data protection and privacy and the possible educational benefits of their products.

Since it is likely that personal data processed by EdTech for both public and commercial purposes will grow in future, we conclude with recommendations for law, policy and practice that respect children's rights and that do not unduly burden schools but support their capacity to determine what is needed for their students. First, as the overall duty bearer and custodian of children's rights in educational contexts, the DfE should work with the ICO to institute robust and trusted processes to ensure compliance with data protection laws and respect the rights of children as data subjects in relation to both public and private sector uses of education data. This could include the development of mandatory or advisory standards and certification schemes. The DfE should also ensure that schools receive the technical and legal guidance they need to procure and contract with EdTech companies in ways that underpin children's education and best interests, informed by up-to-date and evidence-based assessments of the educational benefits (or otherwise) of EdTech on the market. Implementing these recommendations should include widespread consultation with schools, children and parents, preferably as part of conducting a Child Rights Impact Assessment (CRIA) (Mukherjee, Pothong, and Livingstone 2021).

Second, the ICO should exercise its mandatory audit power to systematically enforce data protection laws on data controllers and processors in the education context to ensure that the DfE, schools and EdTech providers fulfil their data protection responsibilities according to their respective roles. It should collaborate with the DfE to develop sector-specific guidance for schools and EdTech providers, including procurement guidance and standard contractual clauses, and possibly build on the DfE's (2018a) Data Protection Toolkit for Schools. It should also act promptly in clarifying the nature of data controllers, the lawful bases of data processing, the application scope of the

AADC, and other technical confusions as they arise, so that schools and EdTech understand their data protection responsibilities.

Third, an EdTech industry body and all providers should act to raise standards regarding both the proven educational benefits of EdTech and their compliance with data protection laws. This could include developing a joint repository of evidence between the British Educational Suppliers Association (BESA) and the DfE, publicly documenting compliance with data protection laws, the HRA 1998 and EA 2010 by publishing DPIA and CRIA which anticipate and evaluate the impact of their product and service after deployment and adhering to the AADC as a matter of good practice.

The combined outcome should empower schools to make decisions about EdTech that align with children's educational needs and best interests and, in return, build trust in technology and EdTech providers. Without such improvements, continued problems with the governance of data processed from children in educational contexts can be expected, as evidenced in the required adjustments to Google G Suite for education in New Mexico (United States District Court for the District of New Mexico 2020) and the Netherlands (Nas and Terra 2021). Such problems, in turn, place pressure on schools and impede their efforts to concentrate on the task of education. Meanwhile, the realisation of children's rights to privacy and education, among other rights, are left to the mercy of the private sector.

Acknowledgements

This work is part of the Digital Futures Commission, funded by the 5Rights Foundation and London School of Economics and Political Science. An earlier version of this work was published as Day (2021) *Governance of data for children's learning in UK state schools* and has been thoroughly reworked for the present submission. The authors would also like to thank the experts and interviewees for their time and insights.

Disclosure statement

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

Funding

This work was supported by Digital Futures Commission - 5Rights Foundation.

ORCID

Emma Day http://orcid.org/0000-0002-9598-6196
Kruakae Pothong http://orcid.org/0000-0002-1735-7941
Ayça Atabey http://orcid.org/0000-0003-3165-6750
Sonia Livingstone http://orcid.org/0000-0002-3248-9862

References

5Rights Foundation. 2021. "Letter to the ICO: Breaches of the Age Appropriate Design Code." *5Rights Foundation*, October. https://5rightsfoundation.com/in-action/letter-to-the-ico-breaches-of-the-age-appropriate-design-code.html.

5Rights Foundation. 2022. "Shedding light on AI: A framework for algorithmic oversight." *5Rights Foundation*, June. https://5rightsfoundation.com/in-action/shedding-light-on-ai-a-framework-for-algorithmic-oversight.html.

Arbuckle, Luk, and Felix Ritchie. 2019. "The Five Safes of Risk-Based Anonymization." *IEEE Security & Privacy* 17 (5): 84–89. doi:10.1109/MSEC.2019.2929282.

Barassi, Veronica. 2020. *Child Data Citizen: How Tech Companies Are Profiling Us from Before Birth*. 1st ed. Cambridge, MA: MIT Press.

Bradbury, Alice. 2019. "Datafied at Four: The Role of Data in the 'Schoolification' of Early Childhood Education in England." *Learning, Media and Technology* 44 (1): 7–21. doi:10.1080/17439884.2018.1511577.

Coughlan, Sean. 2020. "Students Warn Mock Grades 'Make Mockery' of Exams." *BBC News*, August 12. https://www.bbc.co.uk/news/education-53746140.

Day, Emma. 2021. "Governance of Data for Children's Learning in UK State Schools." *Digital Futures Commission, 5Rights Foundation*, June. https://digitalfuturescommission.org.uk/wp-content/uploads/2021/06/Governance-of-data-for-children-learning.pdf.

DCMS (Department for Digital, Culture, Media & Sport). 2020. "Safer Technology, Safer Users: The UK as a World Leader in Safety Tech". May 27. https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech.

DCMS (Department for Digital, Culture, Media & Sport). 2021. "National Data Strategy Mission 1 Policy Framework: Unlocking the value of data across the economy". November 24. https://www.gov.uk/government/publications/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy.

Desai, Tanvi, Felix Ritchie, and Richard Welpton. 2016. "Five Safes: Designing Data Access for Research." *University of the West of England - Economics Working Paper Series* 1061. doi:10.13140/RG.2.1.3661.1604.

DfE (Department for Education). 2017. "DfE External Data Shares". Accessed 10 February 2022. https://www.gov.uk/government/publications/dfe-external-data-shares.

DfE (Department for Education). 2018a. "Data Protection: A Toolkit for Schools." Accessed 10 February 2022. https://www.gov.uk/government/publications/data-protection-toolkit-for-schools.

DfE (Department for Education). 2019. "Realising the Potential of Technology in Education: A Strategy for Education Providers and Technology Industry." Accessed 10 March 2022. https://www.gov.uk/government/publications/realising-the-potential-of-technology-in-education.

DfE (Department for Education). 2020. "Hardware - Education & Pupil Devices." Accessed 15 February 2022. https://www.contractsfinder.service.gov.uk/notice/e9047eeb-be82-4506-8a97-448ff0d73cfe?origin = SearchResults&p = 1.

DfE (Department for Education). 2021a. "DfE's Digital and Technology Strategy". Accessed 30 September 2022. https://dfedigital.blog.gov.uk/2021/04/21/strategy/.

DfE (Department for Education). 2021b. "Data Protection: How we Share Pupil and Workforce Data." Accessed 30 September 2022. https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data#why-we-share-data.

DfE (Department for Education). 2021c. "Transparency Data - DfE External Data Shares" Accessed 30 January 2022. https://www.gov.uk/government/publications/dfe-external-data-shares.

DfE (Department for Education). 2022a. "Guidance - How to Access Department for Education Data Extracts." Accessed 30 September 2022. https://www.gov.uk/guidance/how-to-access-department-for-education-dfe-data-extracts.

DfE (Department for Education). 2022b. "The Complete School Census." Accessed 16 February 2022. https://www.gov.uk/guidance/complete-the-school-census.

DiCerbo, Kristen. 2016. "Integrating Data Across Digital Activities." *Learning, Media and Technology* 41 (2): 233–251. doi:10.1080/17439884.2014.950587.

European Data Protection Board. 2020. "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 (Adopted on 20 October 2020)." https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

European Parliament. 2015. "Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.".

European Union. 1957. 'Treaty Establishing the European Community (Consolidated Version'), *Rome Treaty*, 25 March 1957.

FFT (Fischer Family Trust) Education Ltd. "FFT Aspire". Government Digital Service. Accessed 15 December 2021. https://www.digitalmarketplace.service.gov.uk/g-cloud/services/539394015349528.

Gellert, Raphael. 2016. "We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection." *European Data Protection Law Review* 2 (4): 481–492. doi:10.21552/EDPL/2016/4/7.

Gil González, Elena, and Paul De Hert. 2019. "Understanding the Legal Provisions That Allow Processing and Profiling of Personal Data—an Analysis of GDPR Provisions and Principles." *ERA Forum* 19 (4): 597–621. doi:10.1007/s12027-018-0546-z.

Gove, Michael. 2012. "Written Ministerial Statements - National Pupil Database." Accessed 10 December 2021. https://publications.parliament.uk/pa/cm201213/cmhansrd/cm121106/wmstext/121106m0001.htm.

Groos, Daniel, and Evert-Ben van Veen. 2020. "Anonymised Data and the Rule of law." *European Data Protection Law Review* 6 (4): 498–508. doi:10.21552/edpl/2020/4/6.

Gulson, Kalervo, Carlo Perrotta, Ben Williamson, and Kevin Witzenberger. 2021. "Should We be Worried About Google Classroom? The Pedagogy of Platforms in Education." *Critical Studies in Education* 62 (1): 97–113. https://cpl.asn.au/journal/semester-2-2021/should-we-be-worried-about-google-classroom-the-pedagogy-of-platforms-in.

Hooper, Louise, Sonia Livingstone, and Kruakae Pothong. 2022. "Problems with Data Governance in UK Schools: The Cases of Google Classroom and ClassDojo." *Digital Futures Commission, 5Rights Foundation*, August. https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf.

IBIS Capital. 2019. "Insights and Research." Accessed 20 November 2021. http://www.ibiscap.com/index.php/insights-research/.

ICO (Information Commissioner's Office). 2022. "Case Reference Number INV/0538/2022." https://ico.org.uk/media/action-weve-taken/4022280/dfe-reprimand-20221102.pdf.

ICO (Information Commissioner's Office). 2019. "Findings from the ICO's Consensual Audits of 11 Multi Academy Trusts." Accessed 26 December 2021. https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618610/mats-outcome-report-v1_1.pdf.

ICO (Information Commissioner's Office). 2020a. "Age Appropriate Design: A Code of Practice for Online Services." 1-117. Accessed 25 December 2021. https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/.

ICO (Information Commissioner's Office). 2020b. "Department for Education: Data Protection Audit Report." Accessed 25 December 2021. https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf.

ICO (Information Commissioner's Office). 2020c. "The Right of Access (Guide to the GDPR))." Accessed 25 December 2021. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/.

ICO (Information Commissioner's Office). 2021a. "FAQs for Education Technologies (edtech) and Schools." Accessed 25 December 2021. https://ico.org.uk/for-organisations/childrens-code-hub/additional-resources/faqs-for-education-technologies-edtech-and-schools/.

ICO (Information Commissioner's Office). 2021b. "Guide to the GDPR." Accessed 25 December 2021. https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf.

ICO (Information Commissioner's Office). 2021c. "What are the Rules about an ISS and Consent?". https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-are-the-rules-about-an-iss-and-consent/#a3.

Komljenovic, Janja. 2021. "The Rise of Education Rentiers: Digital Platforms, Digital Data and Rents." *Learning, Media and Technology* 46 (3): 1–13. doi:10.1080/17439884.2021.1891422.

Kurni, Muralidhar, and K. G. Srinivasa. 2021. "Introduction to Learning Analytics." In *A Beginner's Guide to Learning Analytics*, edited by Dirk Ifenthaler David Gibson, 1–28. Cham: Springer International Publishing.

Landau, Susan. 2018. "Understanding Data Breaches as National Security Threats." In *Lawfare*, February 26. https://www.lawfareblog.com/understanding-data-breaches-national-security-threats.

Lievens, Eva, and Ingrida Milkaite. 2018. "Towards a Better Protection of Children's Personal Data Collected by Connected Tous and Devices." *Digital Freedom Fund*. Accessed 25 December 2021. https://digitalfreedomfund.org/towards-a-better-protection-of-childrens-personal-data-collected-by-connected-toys-and-devices/.

Lindeblad, Emma, Staffan Nilsson, Stefan Gustafson, and Idor Svensson. 2017. "Assistive Technology as Reading Interventions for Children with Reading Impairments with a one-Year Follow-up." *Disability and Rehabilitation: Assistive Technology* 12 (7): 713–724. doi:10.1080/17483107.2016.1253116.

Livingstone, Sonia, Kruakae Pothong, and Ayça Atabey. 2021. "Addressing the Problems and Realising the Benefits of Processing Children's Education Data: Report on an Expert Roundtable." *Digital Futures Commission, 5Rights Foundation*, November. https://digitalfuturescommission.org.uk/wp-content/uploads/2021/11/Roundtable-report-25112-final.pdf.

Livingstone, Sonia, and Julian Sefton-Green. 2016. *The Class: Living and Learning in the Digital Age*. New York: NYU Press. https://doi.org/10.18574/nyu/9781479884575.001.0001.

Luckin, Rosemary, and Mutlu Çukurova. 2019. "Designing Educational Technologies in the age of AI: A Learning Sciences-Driven Approach." *British Journal of Educational Technology* 50 (6): 2824–2838. doi:10.1111/bjet.12861.

Lynch, Paul, Nidhi Singal, and Gill A. Francis. 2021. "EdTech for Learners with Disabilities in Primary School Settings in LMICs: A Systematic Literature Review." *EdTech Hub*, March. https://doi.org/10.5281/zenodo.4348995.

Lynskey, Orla. 2015. *The Foundations of EU Data Protection Law, Oxford Studies in European Law*. 1st ed. Oxford: Oxford University Press.

Macfadyen, Leah P., and Shane Dawson. 2012. "Numbers Are Not Enough. Why e-Learning Analytics Failed to Inform an Institutional Strategic Plan." *Educational Technology & Society* 15 (3): 149–163. https://www.proquest.com/scholarly-journals/numbers-are-not-enough-why-e-learning-analytics/docview/1287024911/se-2.

Macgilchrist, Felicitas. 2019. "Cruel Optimism in Edtech: When the Digital Data Practices of Educational Technology Providers Inadvertently Hinder Educational Equity." *Learning, Media and Technology* 44 (1): 77–86. doi:10.1080/17439884.2018.1556217.

Mascheroni, Giovanna, and Andra Siibak. 2021. *Datafied Childhoods, Data Practices and Imaginaries in Children's Lives*. New York, United States of America: Peter Lang Verlag.
Minister for the Cabinet Office acting through Crown Commercial Service. 2021. "Cloud Compute." May 21. https://www.find-tender.service.gov.uk/Notice/011421-2021?origin = SearchResults&p = 1.
Mukherjee, Sudeshna, Kruakae Pothong, and Sonia Livingstone. 2021. "Child Rights Impact Assessment: A tool to realise children's rights in the digital environment." *Digital Futures Commission, 5Rights Foundation*, March. https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf.
Nas, Sjoera, and Floor Terra. 2021. "Google Workspace DPIA for Dutch DPA." *De Rijksoverheid Voor Nederland*, February 12. https://www.rijksoverheid.nl/documenten/publicaties/2021/02/12/google-workspace-dpia-for-dutch-dpa.
National Cyber Security Centre. 2021. "Alert: Further Ransomware Attacks on the UK Education Sector by Cyber Criminals." Accessed 16 December 2021. https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector.
Nottingham, Emma, Caroline Stockman, and Maria Burke. 2022. "Education in a Datified World: Balancing Children's Rights and School's Responsibilities in the age of Covid 19." *Computer Law & Security Review* 45: 105664. doi:10.1016/j.clsr.2022.105664.
ONS (UK Office for National Statistics). 2020. "The Five Safes (Accessing secure research data as an accredited researcher)." Accessed 5 April 2021. https://www.ons.gov.uk/aboutus/whatwedo/statistics/requestingstatistics/approvedresearcherscheme#the-five-safes.
ONS (UK Office for National Statistics). 2021. "ONS Research and Data Access Policy." Accessed 20 December 2021. https://www.ons.gov.uk/aboutus/transparencyandgovernance/datastrategy/datapolicies/onsresearchanddataaccesspolicy.
Persson, Jen. 2020. "The State of Data 2020: Mapping a Child's Digital Footprint Across England's State Education Landscape." *defenddigitalme*. Accessed 25 December 2021. https://defenddigitalme.org/research/the-state-of-data-2020/report/.
Peters, Najarian. 2022. "Black Data Traditions and the Praxis of Childhoold Preservation and Anti-Subordination in Education in the USA and the UK." In *Education Data Futures: Critical, Regulatory and Practical Reflections*, edited by Sonia Livingstone, and Kruakae Pothong, 113–125. London: Digital Futures Commission, 5Rights Foundation.
Ritchie, Felix. 2017. "The 'Five Safes': A Framework for Planning, Designing and Evaluating Data Access Solutions." *Data for Policy 2017: Government by Algorithm?*. London. doi:10.5281/ZENODO.897821.
Samek, Wojciech, and Klaus-Robert Müller. 2019. "Towards Explainable Artificial Intelligence." In *Explainable AI: Interpreting, Explaining and Visualizing Deep Learning*, edited by Wojciech Samek, Grégoire Montavon, Andrea Vedaldi, Lars Kai Hansen, and Klaus-Robert Müller, 5–22. Cham: Springer International Publishing.
Selwyn, Neil. 2015. "Data Entry: Towards the Critical Study of Digital Data and Education." *Learning, Media and Technology* 40 (1): 64–82. doi:10.1080/17439884.2014.921628.
Selwyn, Neil, Luci Pangrazio, and Bronwyn Cumbo. 2021. "Attending to Data: Exploring the use of Attendance Data Within the Datafied School." *Research in Education* 109 (1): 1–18. doi:10.1177/0034523720984200.
Siemens, George, and Phil Long. 2011. "Penetrating the fog: Analytics in Learning and Education." *EDUCAUSE Review* 46 (5): 31–40. https://er.educause.edu/articles/2011/9/penetrating-the-fog-analytics-in-learning-and-education.
Silberman, Roxane. 2021. "Developing Access to Confidential Data in France: Results and new Challenges." *Journal of Privacy and Confidentiality* 11 (2): 1–8. doi:10.29012/jpc.788.
Smith, Helen. 2020. "Algorithmic Bias: Should Students pay the Price?" *AI & SOCIETY* 35 (4): 1077–1078. doi:10.1007/s00146-020-01054-3.
Stoilova, Mariya, Sonia Livingstone, and Rishita Nandagiri. 2020. "Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy." *Media and Communication* 8 (4): 197–207. doi:10.17645/mac.v8i4.3407.
Stringer, Eleanor, Cathy Lewin, and Robbie Coleman. 2019. "Using Digital Technologies to Improve Learning: Guidance Report." *Education Endowment Foundation*. https://educationendowmentfoundation.org.uk/public/files/Publications/digitalTech/EEF_Digital_Technology_Guidance_Report.pdf.
Turner, Sarah, Kruakae Pothong, and Sonia Livingstone. 2022. "Education Data Reality: The challenges for schools in managing children's education data." *Digital Futures Commission, 5Rights Foundation*, June. https://digitalfuturescommission.org.uk/wp-content/uploads/2022/06/Education-data-reality-report.pdf.
UK Data Service. 2022. "What is the Five Safes framework." *SecureLab*. Accessed 17 February 2022. https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/.
Ungoed-Thomas, J. 2022. "'Woeful' DfE blamed as betting firms gain access to children's data." Accessed 30 November 2022. https://www.theguardian.com/education/2022/nov/06/woeful-dfe-blamed-asbetting- firms-gain-access-to-childrens-data.
UNICEF. 2021. "Effectiveness of Digital Learning Solutions to Improve Educational Outcomes: A Review of the Evidence." *UNICEF*, April 1. https://www.unicef.org/documents/effectiveness-digital-learning-solutions-improve-educational-outcomes.

United States District Court for the District of New Mexico. 2020. "State of Mexico, ex rel., Hector Balderas, Attorney General of the State of New Mexico v. Google LLC (20 February)." https://cdn.vox-cdn.com/uploads/chorus_asset/file/19734145/document_50_.pdf.

van der Hof, Simone. 2018. *Children and Data Protection from the Perspective of Children's Rights - Some Difficult Dilemmas Under the General Data Protection Regulation*. Belgium: Wolters Kluwer.

Veale, Michael. 2022. "Schools Must Resist big EdTech- but it Won't be Easy." In *Education Data Futures: Critical, Regulatory and Practical Reflections*, edited by Sonia Livingstone, and Kruakae Pothong, 67–78. London: Digital Futures Commission, 5Rights Foundation.

Walters, Robert. 2021. "EdTech: the Hyper-Accelerator." In *Robert Walters Tech Series*. https://www.robertwalters.co.uk/hiring/campaigns/edtech-report.html.

Williamson, Ben. 2021. "Google's Plans to bring AI to Education Make its Dominance in Classrooms more Alarming." *Fast Company*, May 28. https://www.fastcompany.com/90641049/google-education-classroom-ai.

Williamson, Ben, and Anna Hogan. 2020. *Commercialisation and Privatisation in/of Education in the Context of Covid-19*. Brussels: Education International Research. https://eprints.qut.edu.au/209028/.

Williamson, Ben, and Nelli Piattoeva. 2019. "Objectivity as Standardization in Data-Scientific Education Policy, Technology and Governance." *Learning, Media and Technology* 44 (1): 64–76. doi:10.1080/17439884.2018.1556215.

Witzenberger, Kevin, and Kalervo N. Gulson. 2021. "Why EdTech is Always Right: Students, Data and Machines in pre-Emptive Configurations." *Learning, Media and Technology* 46 (4): 1–15. doi:10.1080/17439884.2021.1913181.