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

By Emma Day, Kruakae Pothong, Sonia Livingstone and Ayça Atabey

In a new open-access journal article, we examine the governance of data processed from children in educational contexts and ask whether this is in children's best interests. Currently there are two different governance regimes for children's education data: UK GDPR which sits alongside the Data Protection Act (DPA) 2018, and the Five Safes framework, a set of principles which enable data services to provide safe research access to data. Our socio-legal analysis found problems with both governance regimes, as detailed in the article. We conclude with three recommendations to improve the governance of chidlren's education data.

Until fifteen years ago, the government only collected education data through the mandatory termly school census, which feeds the National Pupil Database (NPD), as required by the Education Act 1996. Due to the growth of the EdTech market, there is now a parallel process for education data collected from school children by the private sector, serving commercial purposes. Both data collection processes are governed by the UK GDPR and DPA 2018. But the census, which now contains many more data points than when it was first introduced, is covered by an additional layer of governance: Five Safes data governance framework, which sets out requirements for those who want to access the NPD.

We argue that while the Five Safes Framework is robust when used as originally intended, Department for Education (DfE) **practice over the past years is not fully consistent with either the Five Safes Framework or sometimes even with data protection laws.** Despite the extra layer of governance the Five Safes Framework provides the NPD in theory, exemptions to this regime appear to have become routine in practice. Initially, the NPD was accessible only by government policymakers or academic researchers following strict data governance protocols. Then, the government opened up the NPD for commercial re-use. Our analysis of documented approved NPD data shares shows that the DfE does not consistently apply the Five Safes Framework because the DfE has shared NPD data that contains "instant" or "meaningful" identifiers through direct file transfers to some commercial companies. These direct file transfers violate the "safe settings" and "safe data" principles of the Five Safes Framework.

In its compulsory audit, the Information Commissioner's Office (ICO) found that the DfE only relied on the Five Safes Framework without requiring Data Protection Impact Assessments (DPIA) to be carried out across all sharing applications and deemed that this approach was designed to offer a "legal gateway to 'fit' the application… rather than assess[ing] the application against a set of robust measures". Later, the ICO reprimanded the DfE, following the misuse of the personal information of up to 28 million children.

Image by johnstocker from vecteezy

Our research further finds that commercial entities are free to process children's education data with even less oversight when they process personally identifiable data obtained directly from children through EdTech products than when they access deidentified data from the NPD. Indeed, processing children's education data by EdTech companies remains problematic for several reasons.

First, it is unfair and inefficient to expect schools to negotiate the terms and conditions of contracts with EdTech companies, including multinational tech giants, especially given the confusion over who is the data controller and the data processor. A clear solution to this David and Goliath situation that we have previously advocated would be the use of government-drafted standard contract terms that schools can rely on when they contract with EdTech companies. This is because many EdTech companies position themselves in their contracts with schools as data processors, identifying schools as data controllers, meaning that schools are ultimately liable for data processing decisions.

Second, lack of guidance on what public task means in the education context burdens schools. Where schools are data controllers, they usually rely on the lawful basis of 'public task'. Since there is no government definition of what the public task of education consists of, including the very purpose of education, schools are left with the burden of defining the parameters for proportionate and necessary data processing in the education context.

Third, EdTech companies often offer optional features over and above those required for their core educational purposes. In these cases, the EdTech company becomes an independent data controller for those non-core purposes and is required to evidence that this data processing is necessary and proportionate. However, there is currently very little oversight over these kinds of determinations made by companies.

Fourth, we argue the Age Appropriate Design Code (AADC) applies to most EdTech products used by schools to deliver remote learning and connect teachers with children and their parents, even though schools procured these services for children to use. There is ongoing confusion as to whether or not the AADC applies to EdTech used in schools. The debate is over when an EdTech product, as information society services likely to be accessed by

children and provided to children via an intermediary like a school, should fall outside of the AADC's scope. Even where EdTech products aren't technically subject to the AADC, it would be unfortunate for a lower standard of protection of children's rights to be applied due to a legal loophole or ICO's interpretation of the law.

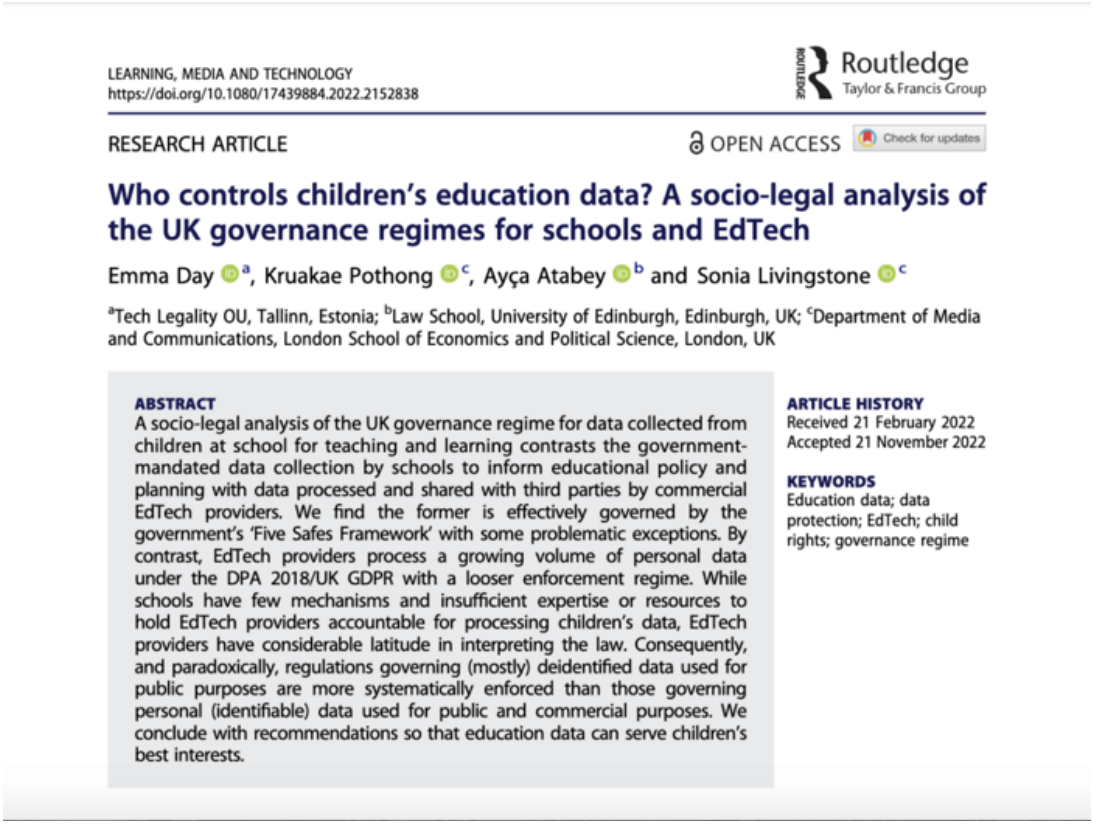
The fifth and most compelling problem we identified is that the government insufficiently implements data protection laws. Despite encouraging EdTech uptake in UK schools and highlighting its benefits for teaching and learning, the DfE has not provided a legally binding EdTech procurement framework or recommended contractual terms, nor endorsed particular EdTech or provided assessment tools for schools to evaluate EdTech on the market.

Overall, 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.

Based on our analysis, we make three key recommendations for law, policy and practice to improve the governance of the use of EdTech in schools:

1. The DfE should work with the ICO to institute robust and trusted processes to ensure compliance with data protection laws and respect children's rights as data subjects concerning both public and private sector uses of education data.
2. 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 responsibilities according to their respective roles.
3. 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.

We hope that the government, as overall duty bearer for children's rights, will empower schools to make decisions about EdTech that align with children's best interests. This would also enable well-founded public trust in EdTech products and provide a more predictable and stable regulatory context for the EdTech sector. Read the full article here.



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