How do our EdTech Certification criteria emerge from our work at the Digital Futures Commission?

By Ayça Atabey, Sonia Livingstone & Kruakae Pothong

After three years of intensive research on the governance of education data at the Digital Futures Commission, we developed a "Blueprint for Education Data: Realising children's best interests in digitised education", a practical framework to tackle EdTech companies violating children's privacy while learning at school.

The Blueprint sets out 10 certification criteria for all EdTech used in schools for teaching, learning, administration and safeguarding. Here we explain the 10 criteria and how they are grounded in our research.

1. Full compliance with the UK Age Appropriate Design Code (AADC)

To identify what a child rights-respecting future for EdTech looks like, we researched EdTech companies' terms of use and privacy policies and their contracts with schools, and interviewed practitioners to explore the gap between what the law says and what happens in practice. We identified a host of problems regarding compliance with the data protection law (e.g., when relying on 'legitimate interests'). In our Governance of data for children's learning in UK state schools report, we called for stakeholders to address these problems, including ensuring full compliance with the UK AADC. We advocated and explained why this is needed in A socio-legal analysis of the UK governance regimes for schools and EdTech among other outputs. Drawing on the expertise of colleagues, we made four proposals to the ICO for developing their framework on children's best interests and have advocated to them that the AADC's standards should be applied to all EdTech.

2. Compliance with privacy and security standards, proportionate to the risks of the data processing, and with the UK government's accessibility requirements

Compliance with the data protection laws isn't sufficient in itself. EdTech companies must comply with other frameworks (e.g.; cybersecurity, equality laws and accessibility requirements), to ensure their data activities are in children's best interests. As we know, privacy matters when enabling a safer online experience for children and the compliance gaps with privacy and security standards that we highlighted in several DFC reports and blogs must be addressed. Accordingly, we trust certification criteria should include compliance with relevant legislation, regulations for data protection, privacy and security, and good practices of risk–benefit calculation.

3. Automatic application and extension of high privacy protection by EdTech to any resources used or accessed as part of a user's digital learning journey by default and design

EdTech companies can better address the best interests of children through data protection by design and by default. Today, not all resources or connected services used provide the same level of protection. To ensure high privacy protection for children's lives, EdTech providers must provide high privacy protection within their own product or service environment and extend the same privacy protection to users' interaction with other products or services accessed through the providers' environment. In this way, children can enjoy consistently high privacy protection throughout their digital learning journey irrespective of the varying privacy protection offered by these other products and services. This privacy extension can be achieved, for example, by creating isolated 'user space' environments which act like containers and apply providers' own privacy policies to these environments.

4. Biometric data is sensitive personal data and must not be processed unless one of the exceptions in the law applies. Children's biometric data and AI-driven technologies are heavily used in educational settings, and the stakes for children are high. As such, children, parents and caregivers must be explicitly notified of the processing of biometric data and given opportunities to provide informed consent. Children and parents must also be able to object to the processing and withdraw the consent given at any time. This is particularly important given that EdTech use can involve pervasive biometric data processing practices which raise legal and ethical questions.

5. Meaningful distinction between factual personal data and inferred or behavioural judgements about children: Maintain a separation between these types of data and do not automate linkages, construct profiles or conduct learning analytics in ways that cannot be disaggregated. Where data are inferred, a clear and transparent account of how the analysis is constructed should be available to the certification body and schools to ensure that behavioural or educational inferences are meaningful and contestable and that transparency rules are respected aligned with their best interests when complying with the data protection laws. Ensuring meaningful distinction is critical given the complexities around connected data for connected services, and how crucial judgments about children can affect their lives and access to services.

6. Opportunities to review and correct errors in the data held about children: Proactively provide prominent, child-friendly and accessible tools for children, parents and caregivers to understand what data is held about the child, enable children and caregivers to review and correct any errors in education records about the child, and provide redress if the errors result in harm. Transparency is key here, because children and caregivers can review any errors if they are informed about what data is held about them. EdTech companies have a responsibility to ensure that they communicate clearly and effectively so that the information can be easily understood and acted upon. Yet, our nationally representative survey showed that less than 1/3 of children reported that their school had told them why it uses EdTech, and fewer had been told what happens to their data or about their data subject rights.

7. Vulnerability disclosure: Provide prominent and accessible pathways for security researchers and others to report any security vulnerabilities of the tools and establish an internal process to promptly act on the reported vulnerabilities. Considering increasing use of EdTech in schools, children's education data is entering the global data ecosystem, and data risks attached to these, addressing vulnerability disclosure standards becomes even more urgent than ever. However, currently there is lack of resources available for those who deal with data protection and security, and provision of prominent and accessible pathways to report and act on security vulnerabilities is needed.

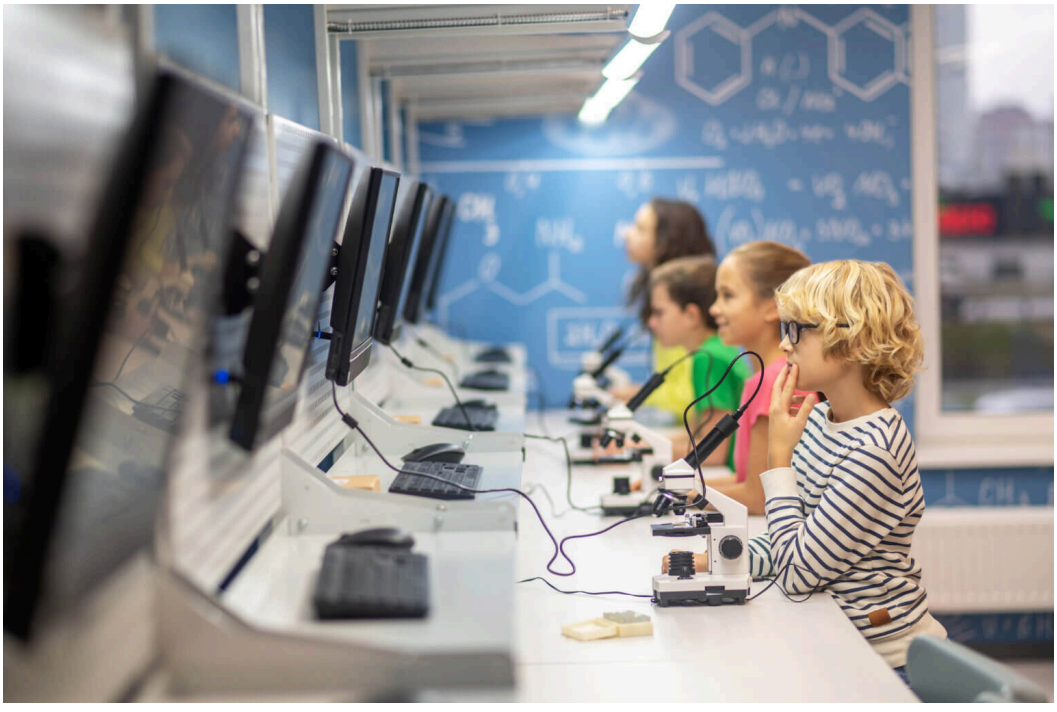

Image by zinkevych from freepik

8. Evidence-based educational benefits: Provide up-to-date peer-reviewed evidence of the benefits of EdTech products, using robust methodologies produced by independent experts free from any conflict of interest. Our expert roundtable report highlighted the lack of evidence about educational benefits. The experts stated that there is a lack of common definitions, evidence or benchmarks for what benefits children in education. Our Education data reality report showed that schools and teachers have similar concerns. Our nationally representative survey results show that children have mixed views about the EdTech products they use in school, and some children doubt the benefits.

9. In-product research: Education data used for R&D by the EdTech provider must meet high ethical and child rights standards. It should not be routine or conducted on children's education data without meaningful informed consent. Our Google Classroom and ClassDojo report shows there is a failure to comply with data protection regulation and this leaves school children vulnerable to commercial exploitation, in many contexts, including in-product research. EdTech providers should respect children's rights and give them control over how their data is used. Fair treatment requires addressing the expectations and needs of children when communicating any information to them for consent. Data-driven education must be responsible, rights respecting, and lawful. In-product research is no exception.

10. Linked services: Ensure service linkages and plug-ins such as in-app purchases that are accessible in EdTech products or services, meet these standards. This criterion requires EdTech providers to ensure that the linked services they choose to offer are compliant with the above criteria by design while the privacy extension in the third criterion addresses privacy protection at the interface level.

Our reports, blogs, and research diagnosed a series of problems with education data governance, which make life difficult for schools and create regulatory uncertainty for businesses and undermine children's best interests. We believe our certification criteria will help to unlock the value of education data in children's interests and the public interest and ensures that children's data aren't exploited for commercial interests in EdTech ecosystem. With children's best interests in mind, we make a clear call to the Department for Education to provide accreditation requirements for EdTech. This should provide clear guidance on the standards to be met and a strong mechanism for implementing this, reducing the burden on schools, creating a level playing field in the industry, and delivering children's rights to privacy, safety and education in a digital world.

Originally posted on https://digitalfuturescommission.org.uk/ on May 22, 2023 .