The state of biometrics 2022: A review of policy in the UK education

Children's biometric data and AI-driven technologies are increasingly used for purposes such as making meal payments and measuring attention, engagement, and emotion in schools. These involve pervasive data processing practices which raise legal and ethical questions.

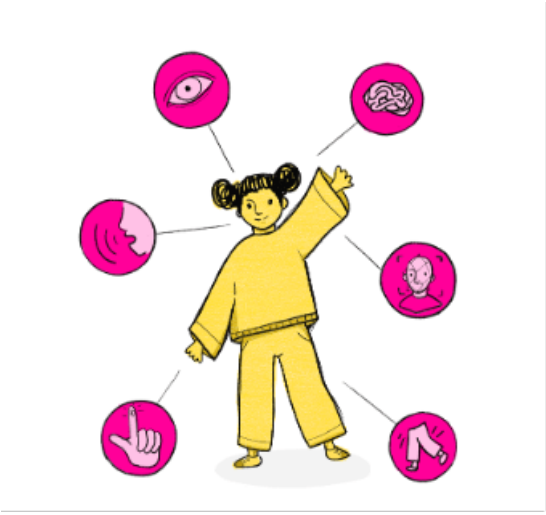
The recent defenddigitalme report, "The State of Biometrics 2022: A Review of Policy and Practice in UK Education", analyses the currently applicable legal framework in the UK. Grounded in practical examples, it questions whether current laws protect children's rights in educational settings where their biometric data is collected. As part of the Digital Futures Commission's commitment to making children's best interests a primary consideration in the design of the digital world, our education data workstream examines uses of pupil data in education settings to develop a child rights-respecting framework for data governance and practice.

What is biometric data?

Building on the definitions set out in the law (namely, Protection of Freedoms Act 2012 (Chapter 2 s.28), UK General Data Protection Regulation (UK GDPR) Article 4(14), Convention 108+ Article 6), defenddigitalme explains biometric data as:

> *"information gathered about a person's physical or behavioural traits that may be used to identify a living person, on its own, or when combined with other personal data of which the data processor is likely to come into possession".*

Biometric data is classified as "special category" data when processed "for the purpose of uniquely identifying a natural person," meaning that as the Information Commissioner's Office (ICO) notes, in many cases, biometric data is special category data. Examples include processing facial images, voice or fingerprint data to charge individual students for their school meals.[1]



defenddigitalme – The State of Biometrics 2022: A Review of Policy and Practice in UK Education

Examples of biometrics used in schools

Biometrics such as facial and fingerprint recognition are used in many different contexts in schools – to reduce problems of cash used in schools such as bullying or theft, promote healthy eating and wellbeing among students, and reduce queues. defenddigitalme's research finds that "from 374 nursery, primary, secondary and sixth forms, a total of 216,296 pupils, 142 schools (38%), 118,445 pupils, were using biometric technology (54%)".

Yet the use of biometric recognition systems has been found to be "unlawful" and schools have stopped using them in several countries (e.g., Poland, France, and Sweden). Some schools in the UK also paused using facial recognition systems following the ICO's inquiries. Aligned with these, defenddigitalme recommends that we should "ban the broad use of biometrics in UK schools".

Image by Peace with Love from Pixabay

Does UK law protect children's biometric data?

The State of Biometrics 2022 argues that "UK Protection of Freedoms Act 2012 and UK data protection laws aren't sufficient to protect children's rights in educational settings". Problematically, the law hasn't kept up with the rapid advance of technologies, "particularly around the use cases in education that sit outside the narrow definition of biometrics for ID purposes". Moreover, defenddigitalme contends that using biometrics leads to discriminatory practices without pupils or parents/carers having a real choice. Yet despite the legal requirement for parental/child consent, biometrics use is obligatory in some UK schools.

What should be done?

defenddigitalme recommends that:

- The ICO should determine that biometric data processing in educational settings in the UK is incompatible with the UK GDPR and Convention 108+ for biometric data and children, upholding the principles of necessity and proportionality.
- All biometric data processing from children for building access, canteen and library uses in educational settings should stop and be replaced by the current non-biometric solutions that must be offered under the Protection of Freedoms Act 2012.
- Legislation should expand to cover technologies that fall outside of "the narrow definition of biometrics for ID purposes".

- Data processing behind the cashless payment systems should be investigated for routine profiling of children's library reading and canteen purchasing habits.
- "The Surveillance Camera Commissioner role should incorporate education where biometrics and surveillance camera systems are utilised under Section 29(6) of the Protection of Freedoms Act 2012".[2]

The EU proposal for Artificial Intelligence Act (AIA)

The EU proposal for a Regulation laying down harmonised rules on artificial intelligence (the proposed Artificial Intelligence Act (AIA)) provides different risk categories and respective obligations and protections under these categories. It also offers additional protections for children. For example, AI systems (like Emotion AI-driven services of a private sector actor) usually fall under a ***lower risk*** category. However, such systems are classified as ***high risk*** in relation to children, as Recital 35 explains:

> *"Children, in particular, constitute an especially vulnerable group of people and require additional safeguards. AI systems intended to shape children's development through personalised education, or cognitive or emotional development should therefore be classified as* ***high-risk*** *AI systems."*

Although the AIA is yet to be finalized, its current version includes specific protections for children in educational settings. Yet the State of Biometrics 2022 shows that the UK's regulatory frameworks and practices lag behind what the AIA proposes for children in the EU. So, we join defenddigitalme in asking: "Will the UK protect children less?" If not, what actions will be taken and when? How do we ensure that these actions have a positive, tangible impact on children's rights in educational settings?

We know that enacting laws can take many years of negotiations (like the GDPR and e-Privacy Regulation). But there is no time to lose in designing rights-respecting digital futures. Personal data – increasingly including biometric data – are heavily used in educational settings, and the stakes for children are high.

Read more about our work on education data here.

Notes:

[1] Article 9 UK GDPR prohibits processing special category data. There are several exceptions to this general prohibition, which are usually called 'conditions for processing special category data'. An example of these conditions/exceptions is "explicit consent". However, note that relying on one of the conditions doesn't necessarily make the processing lawful. For example, in a case where the school based the processing on consent, the Swedish DPA considered that "consent was not a valid legal basis given the clear imbalance between the data subject and the controller".

[2] defenddigitalme adds "While noting that the Act does not apply in Scotland and Northern Ireland, and the current DCMS proposals to reform the role."

Originally posted on https://digitalfuturescommission.org.uk/ on July 18, 2022 .