Biometrics in schools briefing

1. Summary

It is inappropriate and unsafe for us to normalise the expectation in children that they must use their bodies in trivial transactions, particularly in situations that are non-consensual, under peer pressure or imbalances of power. Especially seen in the context of the importance of children understanding consent, in the *Everyone's Invited*[1] work in schools.

If we deviate from the GDPR and regulatory decisions made in other countries it suggests we have a lower standard of data protection than expected in the EU. The disregard for legislation dealing with children's data undermines the value of the DPA 2018 and comparisons for UK - EU GDPR adequacy. Children's rights are protected under various legislation to which countries in the UK are signatories.

What we accept in the UK sends a message to industry and governments worldwide as acceptable practice regards children and biometrics. Our inaction here will be used to undermine children's rights in other places. Should children ever need to use biometrics in schools at all? Biometrics should never be considered necessary or proportionate for tasks children have to do; borrowing school library books or buying snacks at break. Today's uses trivialise biometric data that may be appropriate in high risk or high security settings, as something children should be expected to trade, simply for a slice of a pizza.

Where do we draw the line?

2. Proposed red lines across UK educational settings

- Prohibition on processing biometric data in canteens and cashless payment systems.
- Prohibition on processing biometric data to borrow library books.
- Prohibition on all processing of biometric data across UK educational settings, with exceptions for accessibility (e.g. eye controls of systems for children with disabilities).
- Call for a moratorium on all biometric technology and use of bodily data in schools until September 2023 or until the Information Commissioner carries out an assessment of the use of children's data across UK educational settings, whichever occurs later. (Face, fingerprints, eye scans, vein and palm scanning, gait and emotional detection and processing.)

3. Four Key Issues

1. Legality. Consent is made invalid by the imbalance of power between the school and data subject. Children cannot consent to what they cannot fully understand and extra protections should be obligatory. The legal test of proportionality and whether it is 'necessary in a democratic society' therefore requires some form of impact or risk assessment. The least intrusive option must be used.

2. The regulatory function of the ICO has failed to regulate widespread adoption of biometrics in schools. The ICO has no data on types of biometrics systems used in schools, hardware and software used, suppliers and schools that are using biometrics. There are no requirements for technical standards or specific registration of biometric system suppliers at the ICO nor the DfE. This means it is a free-for-all which companies, from which countries, can get their products introduced into the UK education system, and gain access to millions of UK children's lives and personal data.

3. Current advice[2] to schools in England and Wales issued by the Department for Education on the use of biometric technology. It is out of date (March 2018). It still cites the Data Protection Act 1998 not the GDPR or UK Data Protection Act 2018, and its contents focus on the Protection of Freedoms Act 2012 and processing fingerprints.

---

[1] BBC (March 2021) Everyone's Invited: Schools abuse helpline and review launched https://www.bbc.co.uk/news/education-56588166

[2] Department for Education Guidance (2018) Protection of children's biometric information in schools https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

4**. Absence of accountability, oversight or redress.** The use of technology must be conducted and held to account within a clear and unambiguous framework of legitimacy and transparency. Article 13 of the ECHR gives people a Right to Redress where their human rights are infringed. Yet for children, at scale, there is no body with accountability or place to turn to seek correction of errors, failures from discrimination or products that do not work, or where a child has their rights harmed.

4. Legislation, Court and Data Protection Authority cases

4.1 UK Data Protection Law

The GDPR recognises that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. (Recital 38)

As a data controller any educational setting must protect pupils' personal data, which includes biometric data, in accordance with the Data Protection Act 2018. Facial recognition technology involves the processing of sensitive biometric data, which is defined as "special category data" under Article 9 of the Act, and is as such, subject to a high level of protection.

In order to process sensitive biometric data, controllers must identify both a lawful basis under Article 6 and a separate condition for processing under Article 9, some of which require additional conditions and safeguards under UK law, set out in Schedule 1 of the DPA 2018. If a purpose can be identified, **it could only be considered a lawful purpose under the DPA if no less intrusive methods could be used to achieve the same aim**. (Articles 6, and 9)

Data protection by design and default (Article 25) means that *"measures [that] shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."* It is very unclear in school-parent-child communications who will have access to which data, for what purposes, and if and how families will be notified when this changes.

4.2 Other case studies in law

4.2.1 Florida: Banned Biometrics in schools in November 2014

https://www.flsenate.gov/Session/Bill/2014/0188/BillText/c2/PDF

See lines 51-66: The bill passed by 113 Yeas to 1 Nay
"(1) An agency or institution as defined in s. 1002.22(1) may not:

(a) Collect, obtain, or retain information on the political affiliation, voting history, religious affiliation, or biometric information of a student or a parent or sibling of the student.

For purposes of this subsection, the term "biometric information" means information collected from the electronic measurement or evaluation of any physical or behavioral characteristics that are attributable to a single person, including fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other physical characteristics used for the purpose of electronically identifying that person with a high degree of certainty.

Examples of biometric information include, but are not limited to, a fingerprint or hand scan, a retina or iris scan, a voice print, or a facial geometry scan."

4.2.2 Sweden: Facial recognition and consent (2020)

Sweden issued its first fine under GDPR[3] as a result of its case. The key finding was that consent was not a valid legal basis given the imbalance of power between the data subject and the controller.

4.2.3 France: Courts and authorities find that facial recognition is not necessary and proportionate

A French court canceled[4] a decision in 2020 by the South-Est Region of France (Provence-Alpes-Côte d'Azur – PACA) to undertake a series of tests using facial recognition at the entrance of two High schools considering that this would be illegal. This is the first decision ever by a French Court applying the General Data Protection Regulation (GDPR) on Facial Recognition Technologies (FRTs). The French data protection authority, the CNIL, ordered high schools in Nice and Marseille to end their facial-recognition programs. The controller had failed to demonstrate that its objectives could not have been achieved by other, less intrusive means.

4.2.4 New York State: Facial recognition and other biometrics (2020)

All biometric technology was suspended in New York State schools until July 2022[5], enacted December 2020, primarily because the FR being introduced created controversy, but the bill also covers other biometric technologies.Privacy group EPIC commented, *"The ban will last for two years or until a study by the State Education Department is complete and finds that facial recognition technology is appropriate for use in schools, whichever takes longer."*

4.2.5 Poland: Biometrics: fingerprints (2020)

In 2020 a school in Poland was fined and banned from using biometric fingerprint technology[6] in the school canteen. The Data Protection Authority found the introduction of fingerprints created an unequal treatment of students, as it favoured students who used biometric identification. The authority considered the use of biometric data, "significantly disproportionate".

4.2.6 Scotland: North Ayrshire (October 2021)

In October 2021 North Ayrshire schools began using facial recognition technology supplied via CRB Cunninghams.[7] Some of the wording in forms sent to families made accepting seem compulsory. A tick-box exercise is not valid where a power imbalance affects the nature of 'freely given' consent conditions.

North Ayrshire put its rollout on pause, on October 22nd, 2021 a week after it began. Sixteen months later the ICO published a letter to North Ayrshire Council "Using FRT in schools" and an accompanying case study.[8] This was not enforcement action but made recommendations. These include findings on the conditions for valid consent: (1) If the pupil or parents/carers refuse to provide their consent, the school must give pupils a genuine alternative to the FRT that is not perceived as detrimental by comparison, and that (2) consent could only be valid if the process had been fully informed and freely given. The ICO investigation of the rollout found it was neither and therefore "was likely unlawful".

---

[3]BBC (2019) Facial recognition: School ID checks lead to GDPR fine. https://www.bbc.co.uk/news/technology-49489154

[4] Christakis, (2020). First Ever Decision of a French Court Applying GDPR to Facial Recognition https://ai-regulation.com/first-decision-ever-of-a-french-court-applying-gdpr-to-facial-recognition/

[5] NY State schools ban https://www.nysenate.gov/legislation/bills/2019/a6787 and EPIC https://epic.org/2020/12/new-york-enacts-law-suspending.html

[6] Poland (2020) Fine for processing students' fingerprints imposed on a school https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en

[7] (Sky News) 2021 27 schools in England using facial recognition to take lunch payments https://news.sky.com/story/27-schools-in-england-using-facial-recognition-to-take-lunch-payments-12439330

[8] Case study: North Ayrshire Council schools - use of facial recognition technology (ICO) January 2023 https://web.archive.org/web/20230201012527/https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv/case-study/

While data protection law is permissive as long as the requirements for the freely given nature of consent are met, and that the data subjects are fully informed about the processing, the ICO also stated that in order for the tests of necessity and proportionality to be met, less intrusive alternatives must be unavailable.

Since less intrusive alternatives must *always* be available to cashless catering systems (listed in the ICO case study: "swipe cards, pin numbers or cash" and in many places students simply state their name) and in order to "consent" you must have a choice, aside from the fact that the Protection of Freedoms Act (excluding Scotland) demands that an alternative is offered in law, the ICO failed to take its position to its explicit logical conclusion that other DPAs have before it (France and Sweden). Consent is an inappropriate basis for biometric data processing in educational settings since pupils can rarely be (or are able to be) fully informed and the power imbalance between families and authority, affects and restricts its freely given nature. If use is never necessary as it must be choice, it therefore can never be lawful.

The ICO statement also went on to say that, "the education authority should be assured that the systems have been trained on a representative data sample, and bias testing conducted." However the regulator failed to address the commercial company involvement, to assess the training data sources or their system's accuracy, or to make any comment on the use of the children's personal data (facial data) for use in the product development and commercial supplier influence and intrusion into children's private and family life. We believe the Regulator failed in its duty in this regard.

4.3 Children's human rights are protected in law

The right to privacy is also enshrined in Article 8 of the European Convention on Human Rights (ECHR). Children's rights were enshrined in Welsh law over ten years ago, under the Rights of Children and Young Persons (Wales) Measure 2011[9] that incorporated the United Nations Convention on the Rights of the Child into domestic law. Since May 2014, the Welsh Ministers must, when exercising any of their functions, have due regard to the requirements of the UNCRC. In Scotland is currently in the process of incorporating the UNCRC into domestic law. Under the UNCRC Article 16: "No child shall be subjected to arbitrary or unlawful interference with his or her privacy." As per Article 16(2), "The child has the right to the protection of the law against such interference."

Facial recognition for the purpose of payment is likely in violation of the Human Rights Act 1998, where the law states that the privacy invasion must be proportionate to the threat, and a potential infringement of rights under the UNCRC and the ECHR.

Furthermore, the UNCRC Committee on the Rights of the Child General comment No.16 (2013)[10] para B(1)(27) says that States should not invest public finances and other resources in business activities that violate children's rights. In order to meet this standard, a human rights impact assessment is required.

5. National oversight of health and safety, quality or legal risks and standards

The EU decisions against using facial recognition in schools were acknowledged by the UK Information Commissioner in their June 2021 report, page 22, 'The use of live facial recognition technology in public places.'[11]

[9] Rights of Children and Young Persons (Wales) Measure 2011 https://www.legislation.gov.uk/mwa/2011/2/contents From May 2014, the Welsh Ministers must, when exercising any of their functions, have due regard to the requirements of the Convention (UNCRC)

[10] The UN Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights https://www2.ohchr.org/english/bodies/crc/docs/CRC.C.GC.16.pdf para B(1)(27)

[11] The Information Commissioner (June 2021) 'The use of live facial recognition technology in public places.' https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

> *"In 2019, data protection authorities (DPAs) in France and Sweden took action against controllers using facial recognition in schools. The Swedish regulator issued a monetary penalty under the GDPR to a local authority which instructed schools to use facial recognition to track pupil attendance. The school had sought to base the processing on consent. However, the Swedish DPA considered that* ***consent was not a valid legal basis given the imbalance between the data subject and the controller****. (our emphasis)*
>
> *"The French regulator raised concerns about a facial recognition trial commissioned by the Provence-Alpes-Côte d'Azur Regional Council, and which took place in two schools to control access by pupils and visitors. The regulator's concerns were subsequently supported by a regional court in 2020. It concluded that free and informed consent of students had not been obtained and* ***the controller had failed to demonstrate that its objectives could not have been achieved by other, less intrusive means.****" (our emphasis)*

The ICO, when asked (FOI request, July 2021) about biometrics in schools and consent, processing, complaints and any action taken by the ICO, responded: "We cannot report on the background of complainants or whether their complaints relate to consent and biometric data. This is because we do not need to routinely report on this type of information for our business purposes.[12]"

We believe that this is a significant gap in oversight, but one that could be addressed with a small change to law. Today, all data controllers must register and pay a fee with the ICO and provide some information about what they do. The existing registration process[13] could simply ask the question, whether it includes biometric data, and if yes, whether the data subjects include children.

A limited number of providers operate at scale across unrelated educational settings. There is a lack of assessment at national level of cumulative risks or forward looking future risks for children at scale from different schools, not done in any single school or authority's privacy impact assessment. While on the one hand the level of due diligence needed is missing in schools to assess the quality, health and safety, legal and human rights questions in procurement, the cost of carrying out any data risk assessment is duplicated at each educational setting in its own procurement process.

No ICO or DfE requirements on technical standards for biometrics in schools, means procurement is a free-for-all which companies, from which countries, can get products into the UK education system. They not only extract children's sensitive personal data at scale, but the business intelligence of how the education systems are operated. This could present not only security risks, but risks to the provision of stable and sustainable systems, upon which the state education has become highly dependent.[14]

6. What others have said

6.1 Scotland's First Minister Nicola Sturgeon

In Ministerial Questions on October 28th the MSP, for North East Fife Willie Rennie, asked what the Scottish government position is on facial recognition in schools. **The First Minister, Nicola Sturgeon, responded that she felt the technologies "do not appear to be proportionate or necessary".**

[12] https://www.whatdotheyknow.com/request/biometric_data_in_education#incoming-1846830

[13] https://ico.org.uk/ESDWebPages/Search

[14] See chapter 7 of our report *The State of Biometrics 2022* https://defenddigitalme.org/research/state-biometrics-2022/#chapter-7

6.2 The Biometrics Commissioner for England and Wales

Fraser Sampson was reported in the FT on October 17th[15] to have said, "**if there is a less intrusive way, that should be used."**

6.3 The Ada Lovelace Institute public participation workshops and poll numbers

The Ada Lovelace Institute's 2019 call for a moratorium on biometric technologies like facial recognition was followed by a survey of public attitudes towards facial recognition, published in the report *Beyond Face Value*.[16] The survey showed that not only did the majority of the UK public want greater limitations on the use of facial recognition, but that a deeper understanding of public perspectives was needed to inform what would be considered as socially acceptable for these technologies. **They commissioned a nationally representative survey of 4,109 adults, undertaken in partnership with YouGov and revealed the majority are opposed to its use in schools (67%).[17]**

According to their public poll of 4,109 adults in 2019, nearly half the public (46%) want the right to opt out of the use of facial recognition technology. **This figure is higher for people from minority ethnic groups (56%), for whom the technology is less accurate.**
The Ada Lovelace Institute recommendations cluster around three issues:

1. Developing more comprehensive legislation and regulation for biometric technologies.
2. Establishing an independent, authoritative body to provide robust oversight.
3. Ensuring minimum standards for the design and deployment of biometric technologies.

6.4 The European Commission draft AI Act bans certain high-risk applications of AI

In a joint opinion published in response, **the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) also call for general ban on any use of AI for automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context**[18]—which *should* include educational settings.

7. Poll of Parents of state school children in 2018 in England

Survation polled 1,004 parents of children aged 5-18 in state education in England on behalf of defenddigitalme in February 2018. Over a third (38%) of those who said their child's school uses biometric technology, said they were not offered a choice of whether to use this system or not.[19] That is despite the law that requires parental consent, the Protection of Freedoms Act 2012.

8. Protection of Freedoms Act 2012 England and Wales

Chapter 2 (26-28)[20] requires that families must be notified and consent obtained without either parents or the child's objection, before processing biometric information. This part of the Act does not apply to Scotland and Northern Ireland. An alternative e.g. PIN or card must be offered in any case in Chapter 2

---

[15] FT (October 2021) Facial recognition arrives in UK school canteens https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9

[16] Ada Lovelace Institute report on public attitudes to facial recognition (2019) https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/

[17] Ada Lovelace Institute https://www.adalovelaceinstitute.org/report/citizens-biometrics-council/

[18] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) June 2021 (ref page 2/3) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

[19] Survation (2018) https://www.survation.com/1-in-4-parents-dont-know-child-signed-systems-using-personal-data/

[20] The Protection of Freedoms Act 2012 https://www.legislation.gov.uk/ukpga/2012/9/section/26/enacted (Applies to England and Wales)

(26)(7) of the Protection of Freedoms Act. Schools adding biometrics to cashless systems may add costs.

9. The direction of travel of UK data protection law

The need for these protections for children and young people is heightened by the growth of facial detection coupled with age verification (AV) at supermarket tills in the UK. But the Westminster government's policy direction is not to increase but reduce the safeguards on human rights, as outlined in the DCMS consultation on changes to the UK Data Protection regime, launched on September 10th 2021, *Data: A new direction*?[21]

Some of the safeguards to be removed, disproportionately affect children and young people. **The Biometrics Commissioner** has objected to proposals **to move his remit to the ICO.** *"The functions of these two important roles are very different. The Biometrics Commissioner role is quasi-judicial and covers police retention and use of DNA and fingerprints, the Surveillance Camera Commissioner role is more strategic in providing oversight of the surveillance of public space by the police and local authorities. Both functions are about much more than upholding data rights. Proposing their absorption by the ICO is to misunderstand the specific nature and importance of both."*[22]

10. Discrimination by age, gender and race

There is widespread recognition of research evidence that facial detection, facial recognition and biometric systems are discriminatory. In 2019, researchers for the U.S Department of Commerce National Institute of Standards and Technology found, "elevated false positives in the elderly and in children; the effects were larger in the oldest adults and youngest children, and smallest in middle aged adults."[23]

> *"children… are disadvantaged …by being excluded by policy, or by encountering higher false negatives. Age itself is a demographic factor as accuracy in the elderly and the young differ for face recognition (usually)* ***and also for fingerprint authentication****. This applies even without significant time lapse between two photographs."*

On gender: "Buolamwini and Gebru's 2018 research concluded some facial analysis algorithms misclassified Black women nearly 35 percent of the time, while nearly always getting it right for white men." However, even if accuracy were to improve, there is no necessity to use biometric systems as part of cashless payment systems which must also operate using alternative methods such as PIN or card.

[21] DCMS consultation Data: a new direction (DCMS) September, 2021 https://www.gov.uk/government/consultations/data-a-new-direction

[22] Biometrics Commissioner (October 2021) Response to the proposals from the DCMS Data A New Direction https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response/press-release

[23] 2019 report for the U.S Department of Commerce National Institute of Standards and Technology (Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects) https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

Annexe. Sample of background research: Freedom of Information requests

Date asked	Authority	Response	Reference
28/07/2021	The Department of Education (Westminster)	The DfE does not hold any information on **standards or specifications of any hardware or software of biometric technology used in UK schools.**	https://www.whatdotheyknow.com/request/biometric_technology_in_schools#incoming-1843851
28/07/2021	The Department of Education (Westminster)	The DfE **does not hold any information about suppliers** that provide biometric technology to schools.	https://www.whatdotheyknow.com/request/biometric_technology_in_schools#incoming-1843851
28/07/2021	The Department of Education (Westminster)	The DfE **does not hold any information about the types of biometrics that are used in schools**. i.e. fingerprints, facial recognition, palm, vein or iris scanning.	https://www.whatdotheyknow.com/request/biometric_technology_in_schools#incoming-1843851
17/9/21	The Department of Education (Westminster)	Nor do we provide advice to providers of such [facial recognition] technology. The department's publication [1]Protection of children's biometric information in schools explains the legal duties schools and colleges have if they wish to use biometric information about pupils. (But fails to mention this is long out of date). 2) Please provide your advice to companies which are providers to schools and schools/ educational establishments wishing to use facial recognition technology. (This would include advice ref GDPR and Data Protection Act 2018). 3) Please advise if you have been approached by any companies wishing to supply facial recognition to schools and provide all communications you have had with them, this includes all communications, i.e. minutes of meetings, letters, emails, video calls, etc	https://www.whatdotheyknow.com/request/facial_recognition_use_in_educat#incoming-1878017 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf The above 'Protection of Children's Biometric Information in schools' is out of date. Last update was March 2018 and cites the DPA 1998 4 times, no update on DPA 2018 and GDPR. Needs updating.
2/9/21 Due Back 4th Nov 2021	Information Commissioner's Office (ICO)	• Advice to companies • Working with companies • Facial recognition hardware and software standards to be used in educational establishments?	https://www.whatdotheyknow.com/request/facial_recognition_in_education#outgoing-1198010
8/9/21	Education Scotland	Government does not have the information [on facial recognition in schools] you have requested.	https://www.whatdotheyknow.com/request/facial_recognition_use_in_educat_2#incoming-1871933