The Secretary of State for Science, Innovation and Technology (DSIT),
the Rt Hon Michelle Donelan

Cc.

The Minister for AI and Intellectual Property, Viscount Camrose
The Minister for Data, Julia Lopez MP
The Minister for Research and Innovation, Andrew Griffith MP
The Minister for Tech and the Digital Economy, Saqib Bhatti MP

The Secretary of State for Education, the Rt Hon Gillian Keegan
Minister for the School System, Baroness Barran MBE

Via e-mail

April 14, 2024

Dear Minister,

We call on you to drop the proposed damaging changes to UK data protection law in the Data Protection and Digital Information Bill. We ask instead, that you better protect children, teachers, and society from data harms today and to build the legislative foundations fit for the future threat models from which individuals and society need appropriate protection.

This Bill is the opposite of everything the government says they stand for in Online Safety legislation. Now is the wrong time to downgrade data rules if the UK is serious about becoming an international "tech super power"[1] and producer and exporter[2] of safe, quality and responsible[3] EdTech in a global online environment without geographical boundaries. That requires public trust and adequacy of equivalent international data standards.

<u>Summary position</u>

1. In principle we support the amendment 146 proposal that would require the Information Commissioner to create a Code of Practice for EdTech, as Stephen Cragg KC mentioned in his Legal Opinion on the Bill , in November 2023 (paras 65-66).[4]
2. While we would welcome this amendment to the Bill on EdTech, our preference is that the regulator would create a code of practice for <u>all</u> pupil data processing including by the Department for Education and across the public sector.
3. Therefore, our summary ask is for the government to drop the Bill, as it makes far wider damaging changes to the current UK data protection regime and on balance will harm children's and student data rights as a whole. The Code of Practice should be created under the existing legislation.

The summary outcomes of the Bill

> *"Overall the Bill is a significant shift away from a rights-based regime towards a set of market standards which treats data as a product."* (Stephen Cragg KC, legal opinion)
>
> *"If the new definition of personal data … is enacted that will also, of course, mean that fewer data of children will be protected under the new law.*" (ibid, paragraph 61)
>
> "*The best way to protect children's data is by the retention or introduction of specific safeguards in legislation. However, there is no doubt in my mind that, additionally, such a code of practice as previously advocated for by DDM would be a useful tool for ensuring that special care is taken when the processing of the personal data of children within the education and social care systems (especially) is under consideration."* (ibid, paragraph 66)

The Bill undermines every one of the seven key data protection principles, lowering today's standards of obligations on lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; confidentiality and security; and accountability.

In doing so, the Bill first removes layers of protections, and then points the way for more commercial and other third-parties to exploit those weak spots to intrude into our lives. It gives exemptions to more data users from the full range of current protections by putting product development on a par with public interest research. This will breach the trust and any social licence[5] with the general public for administrative data processing and public interest research, highlighted as vital from public engagement over the last decade that found consistent "red lines"[6] exist when it comes to public acceptability of commercial data reuse.

These changes go to the heart of all data protection legislation, and undermine the very essence of what data protection law is for; to prioritise the protections of the person from arbitrary interference in their private and family life and ensure people have agency by knowing who knows what about them and how that informational power affects our everyday lives. This Bill takes back control not *for* us, but *from* us.[7]

1. **If the new definition of personal data is enacted, children's data will be less well protected under the new law.** The proposed change to the definition of 'personal data' in the Bill means that some data currently defined as 'personal' will in future be excluded from protections everyone has today in the Data Protection Act 2018 and UK GDPR, and fewer data of children will be protected.
2. The terms 'scientific research' and 'scientific research purposes' would now be defined by clause 2 of the Bill to mean **'any research that can *reasonably* be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity**'. This reduces when people can exercise their rights to see a copy of the data, ask for corrections, object to re-uses and it can result in reduced data security when data is kept indefinitely in fully identifiable formats, and not anonymised as it should be now.
3. **Loosening the requirements on purpose limitation** is a seismic shift away from one of the most important principles of data protection law. Undermining this core of protections in

Clauses 3 and 6 means it will be easier to do more unexpected things with our information without informed consent[8] and therefore less protection from re-uses we disagree with.

4. **A list of 'legitimate interests' has been elevated to a position where the fundamental rights of data subjects (including children) can effectively be ignored** where the processing of personal data is concerned. The Secretary of State can add to this list without the need for primary legislation, bypassing important Parliamentary controls.
5. Business friendly interests, such as direct marketing, are now listed without provisos as interests which may be seen as 'legitimate' giving succour to commercial organisations to increase levels of spam, but **without any added safeguards for protection from it for people.** Children are entitled to protection from economic exploitation under Article 32 of the UNCRC, and to inclusive and equitable education opportunities[9] without discrimination.
6. **The changes in Schedule A1 that would permit targeted political marketing at children aged 14-18, may open the floodgates to send children "a deluge"[10] of email direct to their inboxes and phones, including political extremism with no fact checking or oversight.** In 2019 Sky News[11] reported that hundreds of ads were shown to 13 to 17-year-olds on Facebook and Instagram, at a time when it was not permitted. The [then, now former] Children's Commissioner described the practice of targeting young people as "irresponsible".
7. **Further changes have high risk potential for detrimental effects for children and their carers**,[12] including DWP powers for bank account surveillance, however our focus here is for education.
8. **Unsafe technology products may be encouraged under the new 'safeguarding vulnerable individuals' umbrella in Annex 1.** Some claim to be able to identify mood and emotions using "pose estimation" based on data from pupils' faces,[13] or are marketed as being able to identify and profile "hidden social-emotional risks".[14] **Many such products that may soon be banned in educational settings under the EU AI Act, will continue to be permitted in UK classrooms, colleges or universities** if marketed under the 'safeguarding' umbrella. Furthermore, the changes mean they could even skip any risk assessment known as 'the balancing test' in future. Yet another protection that will fall away, encouraging more high-risk products into that unregulated space.
9. Clause 14 does not offer children any protections from automated decision making. **Opaque, unfair algorithms and automated decisions can have life changing outcomes without clear routes for redress**, as students found in the summer exams of 2020.[15] Others have experienced discrimination and little regard for their human dignity when it comes to obligations to use exam remote proctoring tools in Higher Education. Routine 'profiling' that consists of any form of automated processing "should not apply to a child" (GDPR Recital 71) so Article 14 of the Bill is entirely **the wrong direction to take for the security of learners' future identity[16] and society.**

<u>Why these changes matter to get right in educational settings</u>

The education sector is a particular environment and children and learners of all ages have additional needs when it comes to respect for their rights. Children have reduced agency and autonomy in education, but the same rights to privacy, and freedom from arbitrary interference with family and home life and correspondence as learners of all ages. Privacy enables their enjoyment of other rights to protection, to freedom of speech, of conscience

and thought, to enable **the free development and expression of an individual's personality, identity and beliefs.**

EdTech, when used, must promote learners' educational outcomes, social development, and human flourishing. But when it does not, the effects can be long lasting.

> "*Inappropriate data processing practices by e-learning platforms, opaque automated decision-making and misuse of learning analytics, risk undermining data protection and privacy rights.* ***In the case of children and youth, this can have significant and long-term social, economic and professional consequences****"*. (ICDPPC, 2018)[17]

There is already rapid adoption by some teachers of a further range of **emerging high risk data processing products** including generative AI. **In the face of foundational AI models, the education sector is challenged how to respond** to the potential for plagiarism[18], threats to academic integrity and from inaccurate, inappropriate, unreliable text generators offering out of date information, and out of context that use pupils' personal data without permission[19] and that are ethically challenging to use in a sustainable way for children's education due to their extreme demands on water,[20] energy[21] and resources.

Companies have no consistent mechanisms today to demonstrate adherence to the obligations to respect, protect and fulfil the rights of the child[22] and schools cannot assess the business sector's impact.[23] There is growing evidence[24] that many tools do not serve the most marginalised well[25] and can further entrench disadvantage. There is no oversight in England of widespread profiling, data mining, marketing,[26] or school data agreements that can leave children and students of all ages open to commercial exploitation. The 2023 UNESCO *Global Education Monitoring Report* called for regulation and appropriate use of technology.[27]

The EdTech sector is 70% start-ups which can commonly fail to meet cybersecurity standards[28] putting users at risk. They are very often products still in development where the company uses the children's data they collect for new product training and development. But developing companies are often unstable. They can be bought out again and again, often by investors without values directly connected to education or pedagogy, and data control transferred in foreign takeovers multiple times in the course of a child's education.[29] This Bill will inevitably encourage a race to the bottom by encouraging lower standards in EdTech imports and exports as some companies will come to see children in the UK as an easy market for data brokering, increasing the volume of spam, and more upselling within EdTech products.

We must avoid making the UK an easy education market to exploit children as free data producers who are used as training data without consent or using the UK's teachers as free digital labour to perpetuate companies' market dominance[30] especially to the exclusion of competition. **With regard to the re-use of national pupil data for AI development, the DfE is reportedly already considering "a number of questions," including data ownership and IP, working with stakeholders to develop a number of AI tools and "what's it worth,"**[31] but without asking parents if we consent to our children being commercialised, or balancing whether their rights and freedoms outweigh product development interests, or offering families and children any opt out. On top of all this data given away[32], there are regularly data breaches[33] today with no real recourse for redress.

In 2018, a poll by Survation commissioned by Defend Digital Me of 1,004 parents of children

in state education found that 1 in 4 parents said they do not know if their child has been signed up to edTech systems using personal data at all.[34] When it comes to children with special educational needs or a disability, 81% of parents said that parental consent should be required to share this data with third parties such as researchers and commercial companies.

This Bill further shifts today's imbalance of power[35] away from school staff, families and learners, by removing today's obligation to have a Data Protection Officer, and reducing the accountability for data processing. These changes are all detrimental and unnecessary and unsuitable for the future we face.

Educational settings today, including thousands of schools and Academy Trusts, are **over exposed to reputational risk and with a disproportionate workload when each separately repeats[36] the necessary due diligence in EdTech procurement from all over the world**. Instead, we could and should be developing data oversight and a support infrastructure in England to reduce duplicated workload in edTech procurement and deployments.

UK schools have been encouraged to trial high risk technologies, from apps that claim to profile and nudge children's mental health, to platforms collecting data about child protection and injuries, personal data created in education is not always about education. Some school technology companies process neurodata,[37] or share covert photographs taken via school webcams in digital risk surveillance tools[38], and company moderators may even process children's' nude or deeply personal images without oversight. AI is used to profile children's classroom behaviour and used to suggest inferences of interests in terrorism and extremism[39].

Facial recognition and biometric technology are now routine for administrative tasks and cashless catering through 'free' product upgrades from fingerprints to facial readers and without clear information on the source of the technology manufacturers and their incentives. While Sweden, France, Poland and Bulgaria have stepped up to defend school children from unnecessary, disproportionate interference from these high risk technologies after regulatory and judicial action, the UK continues costly mistakes at scale.[40]

In addition to biometric data, increasingly sensitive bodily data are collected by emerging technologies through haptics, immersive tech, robot sensors and by voice assisted tools.[41]

The Department for Education and Government Office for Science recently awarded a contract[42] to look at the implications of future genomic technologies on the education sector too. Some researchers want to see genetic data population-wide joined with educational records, but have no intention of asking first.[43] This Bill is not preparing us for that and the strong societal safeguards it requires, but does the opposite. Dr. Helen Wallace, Director of GeneWatch UK has said of the Bill as drafted[44]

> *"This is a short-sighted and extremely dangerous attempt to tear up existing safeguards for people's DNA and genetic information. If passed, these changes will damage people's trust in health, research and police uses of their DNA, perhaps for generations".*

While the Prime Minister has recognised the potential digital threats to systems and societies and the machinery of democracy through "misinformation and deception of populations", this Bill is the very opposite of what is needed to support and to educate

children and teachers, and to empower individuals with agency and to promote digital competencies.

A vision for the way forward

We believe in the principles of the right to education as set out in universal agreements underpinned by law, that every child has the right to a safe, open, and inclusive[45] education that enables their full and free development into adulthood in a democratic society.[46] Education, as set out in Article 26 of the Universal Declaration of Human Rights, "*shall be directed to the development of the human personality and to the strengthening of respect for human rights and fundamental freedoms, and it shall promote understanding, tolerance and friendship among all nations, racial or religious groups, and shall further the activities of the United Nations for the maintenance of peace*".[47]

Imagine a fair and open market in which safe tools were supported that were effective, equitable, and proven to meet high standards. Better accessibility, pedagogy and trustworthy technologies where businesses and the state are accountable for their designs and decision making.

Imagine moving away from systems that syphon off personal data and with it all the knowledge about the state education system—using teachers' and lecturers' time and work invested in using the product for corporate benefit—and instead the adoption of technology focussed on children's needs and that transparently benefits the public interest.

Imagine decentralised, digital tools that worked together across a child's school day centred on the child's education rather than a series of administrative tools that are rarely interoperable and most often siloed.

Imagine a joined-up vision for a whole curriculum approach, underpinned by pedagogy and proven child outcomes with a safe and secure national infrastructure behind the delivery of state education with a sustainable future state ability to afford, control, and shape it.

We can imagine too, the infrastructure for families' democratic involvement[48] to enable and enforce expectations between schools and families in decisions and data sharing that affect their child from the introduction of technology in education, down to the procurement and installation of CCTV in school bathrooms.

The government must commit to establishing a Code of Practice in educational settings[49] and its enforcement and can do so underpinned by *existing* data protection laws. This should address all data processing across the sector including statutory administrative data collections. The DfE should further consult on dedicated education legislation that will offer clarity, consistency and confidence to educational settings and industry, support staff training and development, and manage learners rights with regard to the quality, safety,[50] and standards of EdTech procurement and outcomes.

We, a non-partisan group of signatories, ask you to uphold today's rights' based framework of data protection law and to drop the damaging changes proposed by this unnecessary rewrite of the UK GDPR.

Signatories

Jen Persson, **Defend Digital Me**.

Dr Patrick Roach, General Secretary, **NASUWT.**

Daniel Kebede, General Secretary, **NEU**.

Leo Ratledge, Co-Director, **Child Rights International Network (CRIN).**

Susannah Copson, Legal and Policy Officer, **Big Brother Watch**.

Jim Killock, Executive Director, **Open Rights Group**.

Tracey Gyateng, **Data Tech & Black Communities** CIC.

Katrina Ffrench, Founder and Managing Director, **UNJUST** CIC.

Sarah Roth-Gaudette, Executive Director, **Fight for the Future.**

Julian Tait, CEO, **Open Data Manchester** CIC.

Ruth Talbot, Founder, **Single Parent Rights**.

Sara Tomlinson, Chair, **More Than A Score**.

Michael Forshaw, CEO, **EdTech Impact**.

Dr Velislava Hillman, Education partner **Etoile Partners and founder of EDDS project**.

Dr Richard Gomer, University of Southampton.

Dr Lyndsay Grant, Lecturer, Education and Digital Technologies Bristol University Digital Futures Institute Affiliate.

Douwe Korff, Emeritus Professor of International Law, London Metropolitan University; Associate, Oxford Martin School; Fellow of the Centre for Internet and Human Rights, Berlin

Dr Sandra Leaton Gray, UCL Institute of Education.

Dr Dan McQuillan, Lecturer in Creative & Social Computing, Goldsmiths, University of London.

Andy Phippen, Professor of IT Ethics and Digital Rights, Bournemouth University.

Ann Phoenix, Professor of Psychosocial studies, UCL

Stephen Tierney, Author and Speaker, Former headteacher, CEO of a Multi Academy Trust and Chair of Headteachers Roundtable (2014 - 2021).

[1] DSIT (March 2023) International Technology Strategy to guide the UK to becoming a tech superpower by 2030. https://www.gov.uk/government/news/plans-to-make-uk-an-international-technology-superpower-launched

[2] DfE (2019) EdTech strategy https://www.gov.uk/government/news/edtech-strategy-marks-new-era-for-schools

[3] Selwyn, N. (2021). Ed-Tech Within Limits: anticipating educational technology in times of environmental crisis. https://bridges.monash.edu/articles/journal_contribution/Ed-Tech_Within_Limits_anticipating_educational_technology_in_times_of_environmental_crisis/14746032

[4] Stephen Cragg (2023) Legal Opinion on the Data Protection and Digital Information Bill commissioned by Defend Digital Me https://defenddigitalme.org/wp-content/uploads/2023/11/KC-opinion-DPDI-Bill-27112023-Stephen-Cragg.pdf

[5] Carter, P., Laurie, G., Dixon-Woods, M. (2015) The social licence for research: why care.data ran into trouble, J Med Ethics 2015;41:404-409 doi:10.1136/medethics-2014-102374

[6] ESRC (2013) Public dialogues on using administrative data https://www.ipsos.com/en-uk/dialogue-data

[7] Already in 2018, 50% of parents asked in a poll by Survation said that they do not have enough control of their child's digital footprint in schools. DDM commissioned Survation to conduct an online poll of 1,004 parents of children aged 5-18 in state schools in England. https://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables-1.pdf

[8] Nesta edTech innovation test bed FAQs: "there is no need for individual consent". https://www.nesta.org.uk/project/edtech-innovation-testbed/frequently-asked-questions/

[9] Article 24 of the UN Convention on the Rights of Persons with Disabilities https://www.allfie.org.uk/campaigns/article-24/

[10] Who Targets Me opinion (2024) Sky News https://news.sky.com/video/voters-targeted-with-political-ads-13081332

[11] Sky News (2019) Teens exposed to highly charged political ads on Facebook and Insta https://news.sky.com/story/teens-exposed-to-highly-charged-political-ads-on-facebook-and-instagram-11786042

[12] Disability Rights UK (2024) Data Protection Bill Proposes "Wholly Unnecessary" Surveillance Measures That Are a "Disproportionate Violation" Of Benefit Claimants Privacy https://www.disabilityrightsuk.org/news/data-protection-bill-proposes-%E2%80%9Cwholly-unnecessary%E2%80%9D-surveillance-measures-are-%E2%80%9Cdisproportionate and BBC (2024) Man 'put through hell' after losing home to DWP https://www.bbc.co.uk/news/uk-england-lancashire-68737244

[13] ViewSonic's myViewBoard Sens Brings UK's First AI-powered Classroom to Smestow Academy https://web.archive.org/web/20230810120916/https://www.viewsonic.com/uk/presscenter/content/viewsonics-myviewboard-sens-brings-uks-first-ai-powered-classroom-to-smestow-academy_4823

[14] Defend Digital Me (2020) See case study 3.10.4 Socio-emotional mental health tracking | Case study STEER AS Tracking https://defenddigitalme.org/research/the-state-of-data-2020/report/

[15] Foxglove (2020) We put a stop to the A Level grading algorithm! https://www.foxglove.org.uk/2020/08/17/we-put-a-stop-to-the-a-level-grading-algorithm/

[16] Human Rights Watch (2023) Data of Tens of Thousands of Students Compromised by UK owned firm https://www.hrw.org/news/2023/04/19/egypt-data-tens-thousands-students-compromised

[17] ICDPPC 2018 resolution on e-learning platforms. 40th International Conference of Data Protection and Privacy Commissioners https://www.edps.europa.eu/sites/default/files/publication/icdppc-40th_dewg-resolution_adopted_en_0.pdf

[18] OpenAI scrapped its detection tool (July 20, 2023) due to low accuracy rate https://openai.com/blog/new-ai-classifier-for-indicating-ai-written-text

[19] DfE guidance on generative tools do not address whether such tools can be used lawfully by pupils (2023) https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education

[20] OECD (2023) Ren, S. How much water does AI consume? The public deserves to know. https://oecd.ai/en/wonk/how-much-water-does-ai-consume

[21] Reuters (2024) OpenAI CEO Altman says at Davos future AI depends on energy breakthrough. https://www.reuters.com/technology/openai-ceo-altman-says-davos-future-ai-depends-energy-breakthrough-2024-01-16/

[22] Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

[23] TES (2010) The sex scandal that took the shine off Sparklebox https://www.tes.com/magazine/archive/sex-scandal-took-shine-sparklebox and see also The UN (2013) General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights https://sites.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf

[24] Human Rights Watch (2023) https://www.hrw.org/news/2022/05/25/governments-harm-childrens-rights-online-learning

[25] Dr. Mwenza Blell, (2023) Data Tech and Black Communities https://digitalfreedomfund.org/the-fight-for-our-digital-rights-to-health-must-be-community-led/

[26] Human Rights Watch, "How Dare They Peep into My Private Life?" – Children's Rights Violations by Governments https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

[27] UNESCO (2023) GEM report https://www.unesco.org/gem-report/en/articles/unesco-issues-urgent-call-appropriate-use-technology-education

[28] Hillman, V. (2022). The state of cybersecurity in education: Voices from the edtech sector. Media & Communications Department Working Paper, London: LSE Department of Media & Communications. Available online: https://www.lse.ac.uk/media-and-communications/assets/documents/research/working-paper-series/WP72.pdf

[29] Case study Edmodo that claimed to have 2 million UK users https://www.edsurge.com/news/2022-08-16-popular-k-12-tool-edmodo-shuts-down

[30] Veale, M. (2023) Schools must resist big EdTech but it won't be easy. https://educationdatafutures.digitalfuturescommission.org.uk/essays/competing-interests-in-education-data/schools-must-resist-big-edtech 5Rights | Digital Futures Commission

[31] Schools Week (2023) Minister wants schools to benefit from AI revolution https://schoolsweek.co.uk/minister-wants-schools-to-benefit-from-ai-revolution/ *and* (2024) DfE Privacy information: development of AI tools https://www.gov.uk/government/publications/privacy-information-artificial-intelligence-ai-tools/privacy-information-development-of-ai-tools

[32] DfE External Data Shares https://www.gov.uk/government/publications/dfe-external-data-shares

[33] Schools Week (2024) ICO launches probe amid reports parents 'saw data of children from other schools' https://schoolsweek.co.uk/reports-of-data-breach-on-class-charts-platform/

[34] Survation (2018) https://www.survation.com/1-in-4-parents-dont-know-child-signed-systems-using-personal-data/ Survation conducted the survey of 1,004 parents of children aged 5-18 in state education in England on behalf of defenddigitalme between 17th-20th February. Full response tables are available to view.

[35] EDPB (2019) Facial recognition in school renders Sweden's first GDPR fine https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

[36] Hillman, V. (2022) Edtech procurement matters: it needs a coherent solution, clear governance and market standards, Social Policy Working Paper 02-22, London: LSE Department of Social Policy.

[37] ICO on neurodata (2023) https://ico.org.uk/media/about-the-ico/research-and-reports/ico-tech-futures-neurotechnology-0-1.pdf

[38] CDT (2023) Report – Beyond the Screen: Parents' Experiences with Student Activity Monitoring in K-12 Schools https://cdt.org/insights/report-beyond-the-screen-parents-experiences-with-student-activity-monitoring-in-k-12-schools/

[39] RSI (2024) Harms caused by 'Prevent' data collection, and surveillance in schools. https://baringfoundation.org.uk/blog-post/uncovering-the-harms-of-prevent-an-update-from-the-work-of-rights-security-international/

[40] ICO letter to North Ayrshire Council on using FRT in schools (2023) https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/01/using-frt-in-schools/

[41] Defend Digital Me (2022) The State of Biometrics https://defenddigitalme.org/research/state-biometrics-2022/

[42] DfE Contract https://www.contractsfinder.service.gov.uk/Notice/3c6eb91c-29a0-4846-bfc4-7713cc8b237f

[43] Farr Institute (2013) https://defenddigitalme.org/wp-content/uploads/2024/03/FarrLondon_maternity.jpg

[44] Genewatch (2024) DPDI Bill briefing http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/dataprot-gw-briefing-fin.pdf

[45] Cranmer, S. and Grant, L. (2022). Can disabled children benefit from education data? In, S. Livingstone and K. Pothong (Eds.), Education Data Futures: Critical, Regulatory and Practical Reflections. Digital Futures Commission, 5Rights Foundation. https://educationdatafutures.digitalfuturescommission.org.uk/essays/seeking-design-solutions/can-disabled-children-benefit-from-education-data

[46] The Right to Education UNCRC Articles 28 and 29 https://www.unicef.org.uk/rights-respecting-schools/the-rrsa/the-right-to-education/

[47] UNDHR Article 26 The Right to Education https://www.un.org/en/about-us/universal-declaration-of-human-rights

[48] Connected by Data (2024) How can affected communities have a powerful voice in shaping the adoption of data-driven technology in schools? https://connectedbydata.org/events/2024-02-26-connected-conversation-edtech

[49] Council of Europe (2020) Committee on Convention 108. Children's data protection in an education setting: Guidelines https://rm.coe.int/prems-001721-gbr-2051-convention-108-txt-a5-web-web-9-/1680a9c562

[50] United Nations Children's Fund (2023) Child Protection in Digital Education: UNICEF Technical Note. https://www.unicef.org/media/134131/file/Child%20Protection%20in%20Digital%20Education%20Technical%20Note.pdf