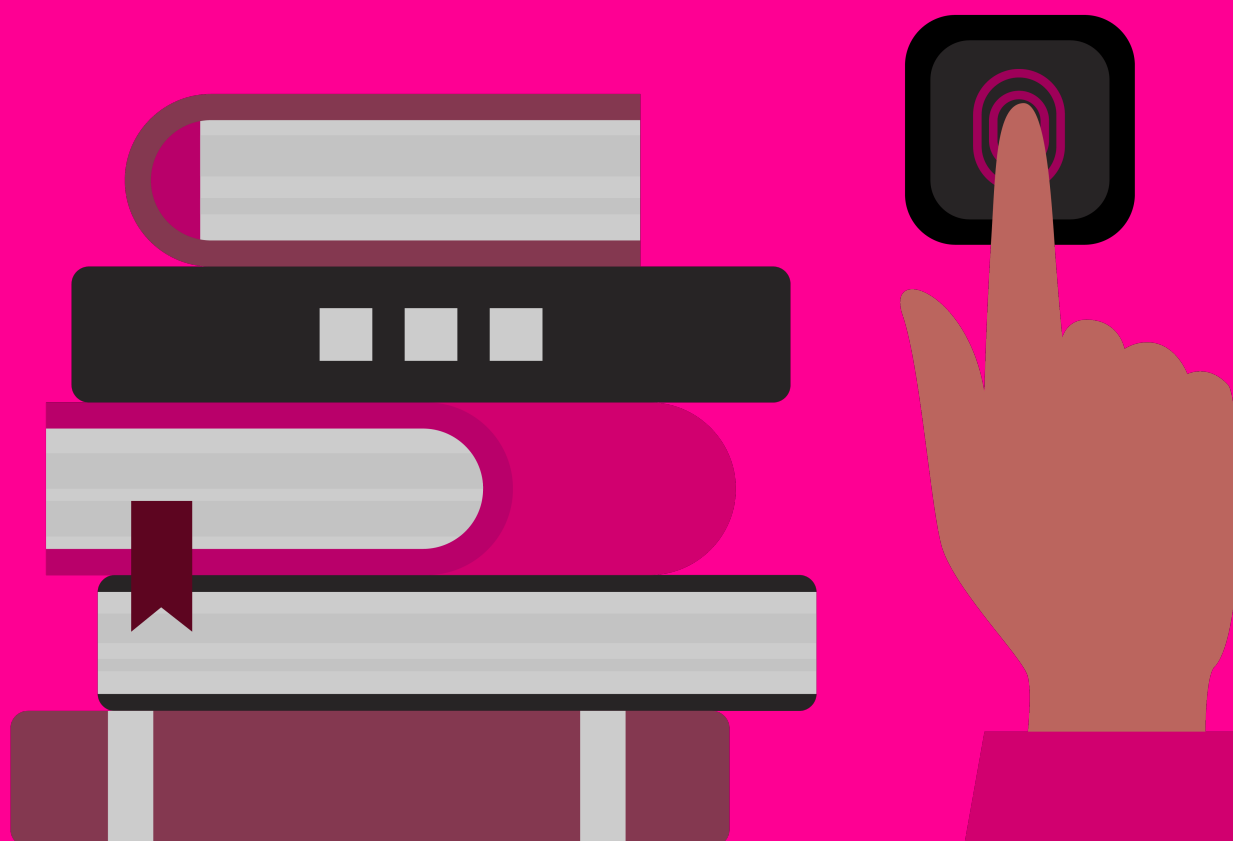


Labels last a Lifetime

Proposals for the creation of a rights respecting environment in education as part of manifesto commitments to children and young people

defenddigitalme



A manifesto for a rights respecting environment in education

“Children do not lose their human rights by virtue of passing through the school gates... Education must be provided in a way that respects the inherent dignity of the child and enables the child to express his or her views freely in accordance with article 12...”

The UN Convention Committee on the Rights of the Child (2001)¹

Policy makers have a duty to respect, protect and fulfil the rights of the child in the digital environment. We recognise that there are challenges in doing this well but the UK is long overdue to make it happen. In the words of Jose Ferreira in 2012², then CEO at the global education platform, Knewton:

“the human race is about to enter a totally data mined existence...education happens to be today, the world's most data mineable industry- by far.”

For a variety of motivations, there is a rapid growth of commercial actors and emerging technologies in the global EdTech market, propagated not only by angel investors and tech accelerators in US and UK English language markets, but across the world. Estimations of market value and investments range widely. One report, ‘*The 2018 Global Learning Technology Investment Patterns: The Rise of the EdTech Unicorns*’, suggested that Chinese EdTech companies were the majority recipients of global EdTech investment in 2018, snapping up 44.1% of a total \$16.34 bn market spend.

At the same time, under global pressure to deliver low-cost state education, and marketisation, the infrastructure to deliver state education is exposed to risks in security and sustainability via commercial ‘freeware’, software that companies offer at no cost, often in a non-explicit exchange for personal data.

The rapid expansion of unregulated educational technology has meant thousands of companies control millions of children’s entire school records. Companies go on to be bought out by angel investors and ownership can be transferred in foreign takeovers multiple times in the course of a child’s education. The child and family may never be told. The school may be forced to accept new terms and conditions without any choice or face losing core system software overnight.

There is no way that a child can understand how large their digital footprint has become or how far it is distributed to thousands of third parties across the education landscape, and throughout their lifetime.

Our research³ shows that school staff, children and parents in England don’t know the National Pupil Database exists, despite it holding the personal confidential records over 21 million named individuals. The ICO has recently agreed (Oct 2019) saying after initial investigation of school census use, that:

“many parents and pupils are either entirely unaware of the school census and the inclusion of that information in the National Pupil Database or are not aware of the nuances within the data collection, such as which data is compulsory and which is optional.”

The ICO complaint on school census (nationality data) 2019⁴

¹ In paragraph 8 of its general comment No.1 on the aims of education

² Jose Ferreira, CEO of Knewton (2012) <https://www.youtube.com/watch?v=Lr7Z7ysDluQ>

³ defenddigitalme research and poll of parents 2018-ongoing <https://defenddigitalme.com/stateofdata2018-gdpr/>

⁴ Outcome on use of complaint against the use of nationality data collected in the school census [case INF0808529]

Families are not told about the onward distribution of personal data from all four National Pupil Databases across the UK⁵. Families are not asked before schools pass their personal confidential data on to hundreds of commercial companies every day. This must change. There must be no surprises how children's personal confidential data are used.

The current government said in its 2019 Education Technology (edTech) strategy, that:

*“The education sector often faces barriers which prevent teachers, lecturers and education leaders benefiting from technology. The UK Education Technology (EdTech) industry also faces barriers to start-up and growth.”*⁶

One person's barriers are another's protections. Innovation need not come at the cost of children's privacy. Children do not have the vote, but do have the right⁷ to have their voices heard.⁸

Government policy across education and administrative datasets should be:

- open, transparent, and responsible,
- courageous, able to make long term decisions beyond short term market fashions,
- co-created. People working in education and families should be consulted on every national expansion of children's personal data extracted across the education sector.

We believe that children in the UK should be:

- treated without discrimination, and are entitled to equal protection under the law with regard to privacy and human rights, and data protection to further human dignity and their best interests.
- empowered to understand according to their capacity, how government and commercial systems affect our lives and know how to seek redress when they disagree with outcomes.
- able to exercise fundamental rights to privacy including opt-out of third-party re-use purposes.
- able to develop into adulthood with a digital clean-slate of public or private storage of data.⁹

While children's agency is vital and they must be better informed of how their own personal data are collected and their digital footprint, there is consensus that children cannot, and should not, be expected to bear the burden of navigating a very complex online environment.¹⁰

The investigative burden in schools at the moment is too great to be able to understand some products, do adequate risk assessment, retrieve the information required to provide to the data subjects, and be able to meet and uphold users' rights. School staff often accept using a product without understanding its full functionality. We need a strong legislative framework to empower staff and companies to know what is permitted and what is not when processing children's data from education and to enable a trustworthy environment fit for the future, so that families can send their children safely to school.

Defenddigitalme
November, 2019

⁵ Comparison of UK national pupil databases https://defenddigitalme.com/wp-content/uploads/2018/05/UK_pupil_data_comparison_May2018.pdf

⁶ DfE national edTech strategy <https://www.gov.uk/government/publications/realising-the-potential-of-technology-in-education>

⁷ 2019 is the 30th anniversary of the founding of the UN Convention on the Rights of the Child <https://www.unicef.org.uk/what-we-do/un-convention-child-rights/>

⁸ Film made for the #MyData2019 conference in Helsinki with @unicef_finland to hear from young people at The Warren Hull and Hiidenkivi High School challenging industry and policy makers on data and privacy <https://defenddigitalme.com/wp-content/uploads/2019/09/DefendDigitalMe-Teaser-v3.0.mp4>

⁹ As recommended by the AI High Level Ethics Group Policy and investment recommendations for trustworthy Artificial Intelligence. “Children should be ensured a free unmonitored space of development and upon moving into adulthood should be provided with a “clean slate” of any public or private storage of data.” <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence>

¹⁰ Stoilova, M., Livingstone, S. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age. <http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline>

Proposed elements for legislation

The UK needs an Educational Rights and Privacy Act to govern the access to educational information and records by commercial companies, public bodies and other third parties, including researchers, potential employers, and on foreign transfers and takeovers.

Clarity, consistency and confidence will be improved across the education sector with a firm framework for the governance and oversight of handling children's personal confidential data.

1. No surprises, through transparency

- Every expansion of national school census collections must have public consultation.
- Start fair communications across the education sector with children and families, telling them annually how their personal confidential data have been used from every school census.
- Companies contracted by schools have an obligation to inform the child/family how their data are used. This applies throughout the life cycle of the data processing, not only at the point of collection, and must be in clear and easy to understand language for a child, in line with data protection legislation. We would design a new framework for managing this through schools.

2. Empower families to take back control under the rule of law

- Develop a legislative framework for the fair use of a child's digital footprint from the classroom for direct educational and administrative purposes at local level, including commercial acceptable use policies. This would deliver clarity, consistency, and confidence to school staff.
- Families must be offered an opt in of school census pupil data third-party reuse.
- Families must be asked for opt in before local authority or other linkage between nursery, primary, and secondary pupil data and data broker records¹¹ or other data provided later in life such as from higher education¹².
- Consider a ban from providing access to identifying pupil personal data collected at the Local Authority and similar level to the national Department for Education or its programs, providers, research partners, governmental bodies, or regulators without explicit parental consent.
- Level up the protections for biometric data across the UK equally to protect children currently not covered in Northern Ireland and Scotland by the Protection of Freedoms Act 2012.

3. Safe data by default

- Stop national pupil data *distribution* for third-party reuse¹³. Enable safe access instead.
- Establish fair and independent oversight mechanisms of national pupil data, so that transparency and trust are consistently maintained in the public sector at all levels.
- Special Educational Needs data such as autism, mental health needs, hearing and sight impairments, and disabilities, must be respected in the same way as health data is in the NHS, in accordance with existing special category data requirements of data protection law.
- The recommendation on persistent identifiers in the International Conference of Data Protection and Privacy Commissioners resolution on e-learning platforms, should be broadly applied, "Consistent with the data minimisation principle, and to the greatest degree possible, the identity of individuals and the identifiability of their personal data processed by the e-learning platform should be minimised or de-identified."¹⁴
- End Home Office access to national pupil data collected for the purposes of education.

¹¹ SATs and scores that last a lifetime (defenddigitalme) March 2019
<https://defenddigitalme.com/2019/03/sats-and-scores-that-last-a-lifetime/>

¹² Statement on student religion and sexual orientation in the National Pupil Database (July 2019)
<https://defenddigitalme.com/2019/07/statement-on-student-religion-or-belief-and-sexual-orientation-data-in-the-national-pupil-database/>

¹³ Requests from organisations to access national pupil databases, and regular external DfE data shares <https://www.gov.uk/government/publications/dfe-external-data-shares>

¹⁴ ICDPPC Resolution on E-Learning Platforms (40th International Conference of Data Protection and Privacy Commissioners (October 2018) https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_dewg-resolution_adopted_en_0.pdf

4. Accountability in public sector systems

- Lawmaking and procurement at all levels of government must respect the UNCRC 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.¹⁵
- Any company processing children's personal data seeking procurement in schools, whether for purchase or as freeware, must demonstrate their accountability for fairness in the design of their technology, as part of that procurement process.
- Introductions of new technology using machine learning, AI, and datasets at scale to require education research ethics committee oversight¹⁶, pedagogical assessment, and publication.

5. Avoiding algorithmic discrimination

- Algorithms can discriminate against young people, women, and ethnic minorities, or indeed anyone based on the bias of the people who build systems and decision making processes.
- Commission an audit of systems and algorithmic decision making using children's data in the public sector at all levels, in particular where linked with education data, to ensure fairness, accessibility, societal impact and sustainability are considered by-design in public policy.

6. A national data strategy fit for their future

- Design a national data strategy built on principles of data justice by design, to establish a trustworthy framework for administrative data use, including education data, in collaboration with all political parties, civil society, industry, local authorities, third-sector, and other experts.
- Recognise children's data merit special protection due to potential lifelong effects.

7. Design for fairness in public data

- Ensure fair and independent oversight mechanisms are established in the control of public administrative datasets, so that transparency and trust are consistently maintained in public sector data at all levels, to deliver comparable insights and equality of outcomes.

8. Accessibility and Internet access

- Accessibility standards for all products used in state education should be defined and made compulsory in procurement processes, to ensure access for all and reduce digital exclusion.¹⁷
- All homes and schools must be able to connect to high-speed broadband services to ensure equality of access and participation in the educational, economic, cultural and social opportunities of the world wide web¹⁸.
- Extend the requirement on basic, affordable telephony to broadband to help ensure every child has adequate access to the Internet and to keep pace with the connected digital economy.
- Ensure a substantial improvement in support available to public and school library networks. CILIP has pointed to CIPFA figures of a net reduction of 178 libraries in England between 2009-10 and 2014-15.¹⁹

¹⁵ General Comment No. 16 (2013) on State obligations regarding the impact of business on children's rights <https://resourcecentre.savethechildren.net/library/general-comment-no-16-2013-state-obligations-regarding-impact-business-childrens-rights>

¹⁶ BERA research ethics (for example) <https://www.bera.ac.uk/publication/ethical-guidelines-for-educational-research-2018-online#consent>

¹⁷ Tackling digital exclusion The Legal Education Foundation (TLEF) director of research and learning Dr Natalie Byrom

¹⁸ See the 'digital' paragraph (April 2019) final report from the All-Party Parliamentary Group for Youth Affairs' inquiry into Youth Work. <https://nya.org.uk/wp-content/uploads/2019/04/APPG-Youth-Work-Inquiry-Final-Report-April-2019-ONLINE.pdf>

¹⁹ Nearly 130 public libraries closed across Britain in the last year (2017-8) and disproportionately affects children Research Library Briefing paper Number 5875, 20 June 2019 <https://www.theguardian.com/books/2018/dec/07/nearly-130-public-libraries-closed-across-britain-in-the-last-year>
<https://defenddigitalme.com/wp-content/uploads/2019/11/SN05875.pdf>

9. Horizon scanning

- Ensure due diligence for safety and ethics are integral in emerging technology markets and in competitive takeovers of products that affect UK school children.²⁰
- Ban the use of facial recognition in schools in line with decisions in France²¹ and Sweden²² and re-assess the use of other biometrics in schools such as fingerprints, given ever-growing risks²³
- Design for age appropriate systems with a consistent, privacy preserving approach to identity.

10. Online harms

- Ensure that children and the most marginalised in society can fully participate in educational, cultural, economic, political, play and other activity online supported by regulation that ensures hate laws and incitement to violence can be acted upon effectively without infringement on participation and freedom of expression, avoiding censorship, or reduction of human rights.
- Promote a rights-respecting digital environment that protects rights to anonymity and identity.

11. Privacy of communications and profiling

- Scale back state surveillance under the Prevent Programme, stopping the mass monitoring of pupils, and collection of communications data, building profiles of individual behaviour.
- Introduce a ban on targeted advertising, using personal information to create profiles about school children, sell or rent their personal data, or onwardly disclose it to further third parties.

12. Security

- Oppose any attempts to undermine encryption and creation of “backdoors” into encryption tools or technology platforms, in order to protect our public data.
- Conduct an education sector audit for outdated infrastructure across mission critical systems that expose the sector to malware.²⁴
- Consider minimum security standards, such as New York’s Student Data law that includes a requirement to encrypt student data in line with the encryption requirements of the federal Health Insurance Portability and Accountability Act (HIPAA) (N.Y. Educ. Law § 2-D(5)(f)(5)).

13. Teacher training

- Introduce data protection and pupil privacy into basic teacher training, to support a rights-respecting environment in policy and practice using edTech and broader data processing, to give staff the clarity, consistency and confidence in applying the high standards they need.
- Ensure ongoing training is available and accessible to all staff for continuous professional development.
- Support at least the same level of understanding across schools, as must be offered to children in developing core curriculum requirements on digital literacy and skills, as recommended by the Select Committee on Communications, in the report, *Growing up with the Internet* (2017).²⁵

²⁰ Edmodo boasted over 2 million accounts in 2016. <https://schoolsweek.co.uk/hackers-steal-edmodo-users-details/> In 2018 China based company, *NetDragon* acquired Edmodo for \$137.5 Million <https://www.edsurge.com/news/2018-04-09-china-s-netdragon-to-acquire-edmodo-for-137-5-million>

²¹ La Cnil juge illégale la reconnaissance faciale à l’entrée des lycées (October 2019) <https://www.mediapart.fr/journal/france/281019/la-cnil-juge-illegale-la-reconnaissance-faciale-l-entree-des-lycees>

²² Supervision pursuant to the General Data Protection Regulation 2016/679 – facial recognition <https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf>

²³ “A high statutory threshold must be met to justify the use of live facial recognition, plus it must demonstrate accountability, under the UK’s data protection law...” (Nov 2019) Information Commissioner’s Opinion from Elizabeth Denham <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/live-facial-recognition-technology-police-forces-need-to-slow-down-and-justify-its-use/>

²⁴ For example, *WannaCry* that caused more than 19,000 appointments to be cancelled, costing the NHS £20m in one week in May 2017 alone, and £72m in the subsequent cleanup.

²⁵ Select Committee on Communications, *Growing up with the internet*, 2nd Report of Session 2016-17 - published 21 March 2017 - HL Paper 130 (para 217) <https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13008.htm>

About defenddigitalme and what we do

defenddigitalme is a call to action to protect children's rights to privacy. We are a non-partisan, non-profit, civil society organisation. We campaign for safe, transparent and fair use of personal confidential data across the education sector in England and beyond. We are funded through an annual grant in 2019-20 from the Joseph Rowntree Reform Trust Ltd.

defenddigitalme | defenddigitalme.com | Registered at Companies House 11831192

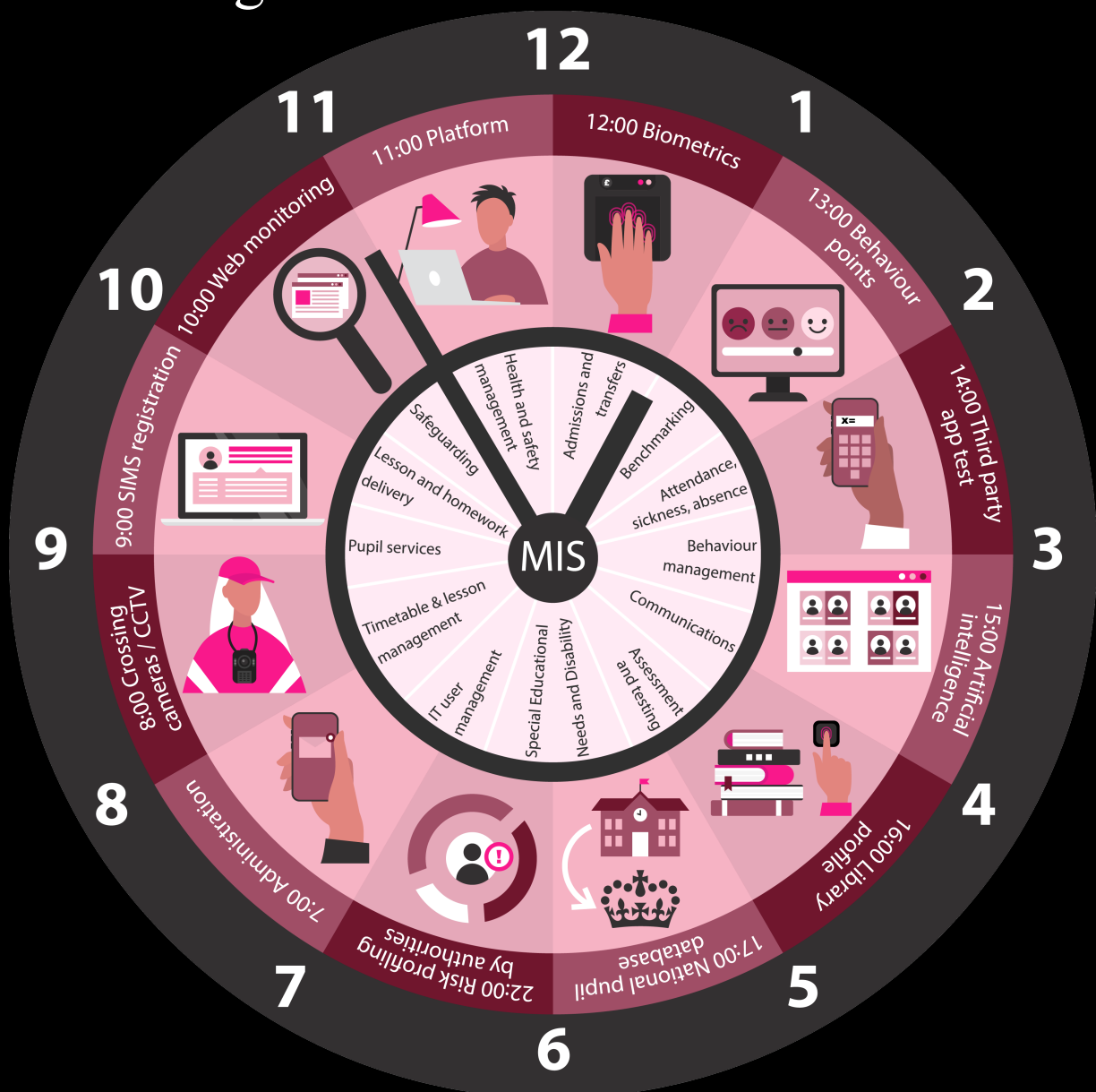
This work is distributed under the terms of the Creative Commons Attribution 4.0 International licence, which permits unrestricted use, distribution and reproduction in any medium, provided the original authors and source are credited.



How was your day?

Can you explain to a child and their family, where a school sends their digital footprint in a single day?

defenddigitalme



myVote2019.uk