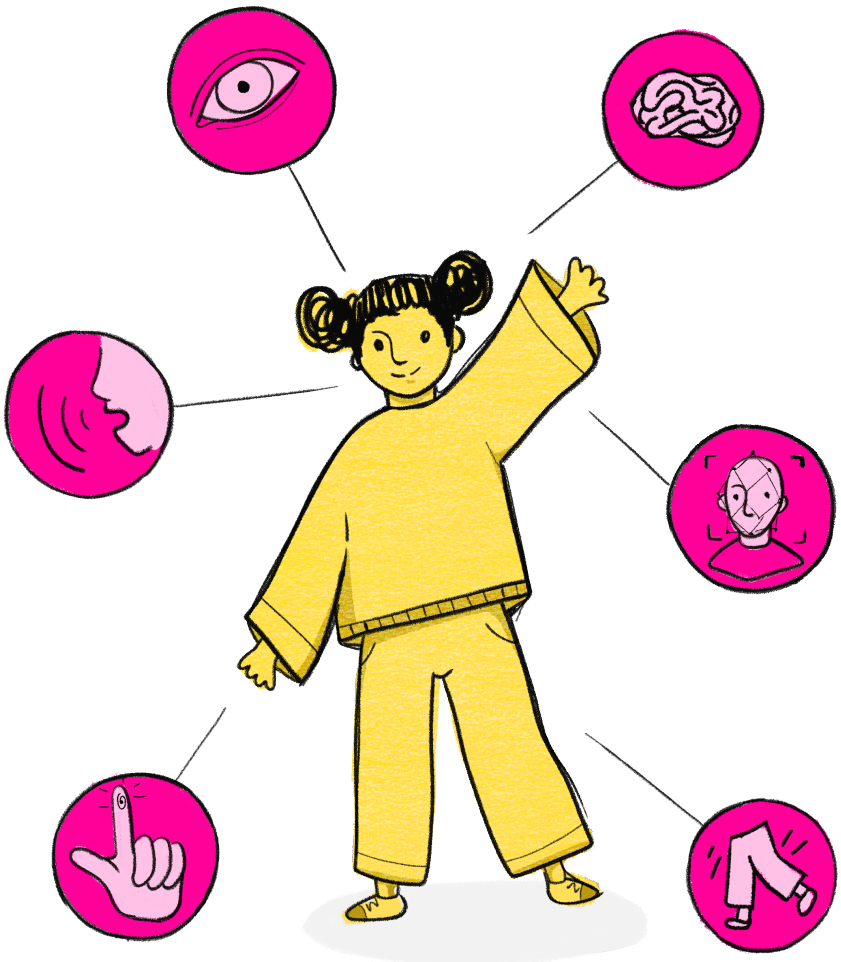
defend|digital|me

Labels last a Lifetime

Commitments for a rights respecting digital environment in state education



May 2024

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. The UK is long overdue to make it happen, especially in the state education system in England. In the words of Jose Ferreira in 2012[2], 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, driven not only by angel investors and tech accelerators in U.S. and UK English language markets, but an appetite for innovation around 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 $16.34bn 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 accelerated in the Covid-19 pandemic and now thousands of companies control millions of children's entire school records. Companies can be bought out and ownership can be transferred in foreign takeovers multiple times in the course of a child's educational lifetime. The child and family may never be told. The school may be forced to accept new terms and conditions without any choice, or even face losing core systems 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. Nearly 1 in 4 parents said in 2018 that they don't know If their child has been signed up to systems using personal data in school in England.[3] Clarity, consistency and confidence must also be improved across the education sector for staff. These recommendations also recognise education is devolved.

When it comes to what the government controls, our research[4] shows that school staff, children and parents in England don't know the National Pupil Database exists, despite it holding the personal confidential records of over 28 million named individuals. The ICO said in 2019 of school census use:

> ***"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) 2019[5]

A consistent rights-based framework[6] and mechanisms to realise children's rights is needed between the child, family and all of the actors in each digital setting; in nurseries and schools, Local Authorities and integrated public services, the Department for Education, companies, and other third-parties for safe, confidential data handling; and to ensure the right to information, accuracy, security and controls.

---

[1] Paragraph 8 of the UNCRC General Comment No.1 on the Aims of Education https://www.ohchr.org/en/resources/educators/human-rights-education-training/general-comment-no-1-aims-education-article-29-2001

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

[3] Survation poll (2018) of 1,004 parents of children in education https://www.survation.com/1-in-4-parents-dont-know-child-signed-systems-using-personal-data/

[4] The State of Data 2020: a mapping of the data landscape in state education in England (2015-20) https://defenddigitalme.org/research/the-state-of-data-2020/

[5] Outcome of Defend Digital Me ICO complaint against the DfE use of nationality data collected in the school census [case INF0808529]

[6] See also: 5Rights Foundation Digital Futures Commission: A blueprint for Education https://digitalfuturescommission.org.uk/beneficial-uses-of-education-data/

Families are not involved in the procurement of new educational technology, not asked before schools pass their personal confidential data on to hundreds of commercial companies or told about the onward distribution of personal data from all four National Pupil Databases across the UK[7]. This must change.There must be no surprises how children's personal confidential data are used. Children have the right[8] to have their voices heard[9] as per their right in the UNCRC, and to trust their digital school life.

The Covid-19 pandemic further demonstrated the key role of reliable and secure infrastructure in education yet there are no safeguards in place for its sustainability. Dependence at scale on industry products such as Information Management Systems, platforms like Microsoft and Google and cashless payment systems, all need risk assessment for both the regular and exceptional delivery of education. We currently operate in the dark. There are risks to state sovereignty to control the curriculum, the purpose and aims of education and teaching of digital citizenship, and the safe and secure delivery of state education should freeware start charging the majority of settings who are dependent upon them.

Government policy across education and administrative datasets should be:

- open, transparent, safe, accountable 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 national expansions of children's personal data extracted across the education sector, and procurement.

We believe that children in the UK should be:

- entitled to equal protection under the law with regard to the full range of human rights;
- empowered to understand, according to their capacity, how ICT and automated systems across education affect their lives, how to make the most of them, and know how to seek redress;
- able to exercise fundamental rights to privacy including opt-out of third-party re-use purposes;
- able to flourish into adulthood with a digital clean-slate of public or private storage of data.[10]

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.[11]

The investigative burden in schools at the moment is also too great for staff or families 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 or security risks[12]. The risks and harms posed by excessive exposure of identifying data and its loss, can last a lifetime. 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.

Legislation, limited infrastructure, and change in practice are needed to manage the digital environment in education. School Information Management Systems (MIS) are already in place to start the process.

An Education and Digital Rights Act should also establish a National Digital Office and the digital infrastructure (via MIS) for secure rights management, to ensure high standards, accountability, staff support and public trust in the digital environment in state education and a child's digital footprint for life.

Defend Digital Me, May 2024

---

[7] Comparison of UK national pupil databases https://defenddigitalme.org/wp-content/uploads/2018/05/UK_pupil_data_comparison_May2018.pdf

[8] The UN Convention on the Rights of the Child https://www.unicef.org.uk/what-we-do/un-convention-child-rights/

[9] Young people from The Warren Hull, and Hiidenkivi High School in Finland challenging industry and policy makers on data and privacy https://defenddigitalme.org/wp-content/uploads/2019/09/DefendDigitalMe-Teaser-v3.0.mp4 Film made for the #MyData2019 conference in Helsinki with Unicef.

[10] 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

[11] 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

[12] BBC May 2024 https://www.bbc.co.uk/news/articles/c2vwz4exq4xo#

Proposed elements for legislation

The UK needs an Education and Digital Rights Act, recognising where necessary the differences in devolved nations, to govern the delivery and access to information and infrastructure management by companies, public bodies and other third parties, including researchers, potential employers, and on foreign transfers and takeovers.

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 and **national statutory data collections from the Early Years through to Higher Education.**
- **Data Rights Management.** Schools have an obligation to inform the child/family how their data are used by EdTech companies contracted by the educational setting. 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 law and findings of the 2020 ICO DfE audit.[13] A new data usage report and notify function for managing this should be **integrated into the existing School Information Management Systems** and parental communications apps, to explain all local data processing including edTech in an annual report.

2. Empower families in a new social contract with the state, 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 control over school census pupil data reuse**.
- Families must be asked for opt in before local authority or other **linkage** between nursery, primary, and secondary pupil data and data broker records[14] or other data provided later in life such as from higher education[15] **beyond direct care** (eg “the NHS data management model”).
- **Extend the protections for biometric data** across the UK[16] equally to protect children currently not covered in Northern Ireland and Scotland by the Protection of Freedoms Act 2012.

3. Safe data access by default to replace outdated data distribution processes

- Enable **safe *access*** to pupil data. **End national pupil data *distribution*** for third-party reuse[17].
- Establish fair an**d 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 the 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*.”[18]
- **End Home Office or DWP[19] access to national pupil data** collected for educational aims.

---

[13] ICO DfE Audit https://defenddigitalme.org/wp-content/uploads/2021/10/department-for-education-audit-executive-summary-marked-up-by-DDM-Jan-2021.pdf

[14] SATs and scores that last a lifetime (defenddigitalme) March 2019 https://defenddigitalme.org/2019/03/sats-and-scores-that-last-a-lifetime/

[15] Does your national school record reveal your sexual orientation or religion? (2023) Defend Digital Me and latest DfE data in answer to parliamentary questions https://defenddigitalme.org/2023/04/02/does-your-national-school-record-reveal-your-sexual-orientation/

[16] The State of Biometrics 2022: A Review of Policy and Practice in UK Education https://defenddigitalme.org/research/state-biometrics-2022/

[17] Requests to access national pupil databases, and regular external DfE data shares https://www.gov.uk/government/publications/dfe-external-data-shares

[18] 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

[19] DWP access to NPD revealed in May 2024 https://defenddigitalme.org/2024/05/10/comment-secret-deal-lets-benefit-fraud-squad-snoop-on-pupil-data/

4. Accountability in public sector systems

- **Establish a National Digital Office (NDO)** to ensure products in state education meet recognised quality and safety standards in pedagogy and effects, before access to the state education system; scrutinise outcomes, and assure public trust and accountability.
- **Legal and regulatory standards need defined to assess the quality of emerging tech.**
- New technology using machine learning, AI, or personal data at scale require **research ethics committee oversight[20], risk assessment, and publication in the open register**.
- 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**[21] and adopt it into UK law.
- Any company processing children's personal data seeking procurement in schools, whether for purchase *or* as freeware, must demonstrate their accountability for safety, accessibility, fairness and equity in the design of their technology, as part of that **procurement process**.
- Freedom of Information laws should be applied to all non-state actors, companies and arms-length government bodies, as pertains to their **role or provision of services in educational and children's state education commissioned by the publicly funded state sector**.

5. Machine fairness: avoiding algorithmic discrimination

- **Commission an audit of systems and algorithmic decision-making using children's data from state education 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. If you don't know where it is or what it is used for, how can we ensure security, accountability, or correctly inform people from whom the data comes?
- **Ban predictive algorithms in high-impact and safety-critical domains** where errors, unreliability, and biases may have life and death consequences e.g. children's social care.
- Ensure **parity of access, protection from discrimination,** and **right to human processing**, to ensure emerging machine applications do not infringe rights e.g in remote exam proctoring.

6. A national data strategy fit for their future

- **Design a national education data strategy** for education to establish a trustworthy framework for administrative data use, including pupil and workforce data, in collaboration with all political parties, civil society, industry, local authorities, unions, third-sector, and other experts.
- Recognise **children's data merit special protection** due to the potential lifelong effects.[22]
- Recognise **unique pupil numbers must lapse** when pupils leave state funded schooling, at the age of 16 or older, and must be a 'blind number' not automatic adjunct to a pupil's name.[23]
- Data linkage may create additional unexpected risks[24] later in life to data collected by previous data controllers. Ensure data minimisation across the lifetime of learners and data lifecycles. Equality monitoring data from students should be statistical not named, at national levels.
- Recommendations on **statutory data collections in the accountability system** are in our State of Data 2020 report: https://defenddigitalme.org/research/the-state-of-data-2020/report/

7. Design for fairness and redress in public administrative education data

- Ensure **fair and independent oversight mechanisms are established at the NDO** in the control of public administrative datasets, to maintain transparency and trust in public sector data at all levels, to deliver comparable insights and equality of outcomes.
- **Enable an effective route for redress in questions of data governance** beyond the school setting **akin to the Caldicott Guardian network** and Office of National Data model in the NHS.

---

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

[21] 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

[22] Resolution from the 2018 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

[23] Guide to the Unique Pupil Number (2019) DfE https://defenddigitalme.org/wp-content/uploads/2024/01/UPN_Guide_1.2.pdf

[24] HE students Equality Monitoring data https://defenddigitalme.org/2023/04/02/does-your-national-school-record-reveal-your-sexual-orientation/

- Oversee **national standards** for the use of public administrative data and linkage in research.

8. Infrastructure, accessibility and inclusion

- **Accessibility standards** and principles[25] for infrastructure and products should be defined and made compulsory in any procurement, to ensure access for all and reduce digital exclusion.[26]
- Schools must be able to access **high-speed broadband services** to narrow the digital divide and participation in the educational, economic, cultural and social opportunities of the web[27].
- Extend the **requirement on affordable telephony to broadband** to ensure every child has adequate access to the Internet **at home** and to keep pace with the connected digital economy.
- Enforce respect in the provision of education in line with the Education Act 1996 s451 **prohibition of charges** for provision of education, as applies in the digital environment.
- Guarantee support available to **public and school library networks.**[28]

9. Horizon scanning for emerging technology and rights' related issues

- **Ensure due diligence** via the NDO for the safety and ethics of products in emerging technology markets and in competitive takeovers of products that affect UK school children.[29]
- **Ban the use of facial recognition in schools** in line with France[30] and Sweden[31] and assess **widespread biometrics practices in schools** such as fingerprints, given ever-growing risk.[32]
- Set out standards for a consistent **privacy preserving approach to identity, user log-ons and family members' access to, in and across education systems, recognising permanent identifiers must lapse on leaving school.**
- **Ensure consistency and fairness** in the approach to the permitted uses of technology in coursework, teaching and learning, marking and assessment, profiling, and data analytics.

10. Online harms

- Ensure that children and those 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 are acted upon effectively without infringement on participation and freedom of expression, **avoiding censorship, or reduction of human rights.**
- **Promote a rights-respecting environment that protects rights to anonymity and identity**.
- Advocate across educational settings to **change practice[33] to stop sharing children's images online in school social media and websites[34]**, widely exposed to data scraping.

11. Privacy of communications and profiling

- **Amend KCSiE to reduce state surveillance** and increase transparency under the Prevent Programme. End the covert mass monitoring of individuals in school settings and at home 24/7 365 days a year and collection of communications data, building profiles of individual behaviour.

---

[25] NASUWT 12 principles for the ethical development and application of artificial intelligence and digital technologies in education https://www.nasuwt.org.uk/advice/in-the-classroom/artificial-intelligence-and-digital-technologies.html

[26] Tackling digital exclusion The Legal Education Foundation (TLEF) director of research and learning Dr Natalie Byrom https://thelegaleducationfoundation.org/articles/the-legal-education-foundation-is-today-publishing-a-blueprint-for-digital-justice

[27] See the 'digital' paragraph (April 2019) final report from the All-Party Parliamentary Group for Youth Affairs' inquiry into Youth Work. (p31) https://nya.org.uk/document/appg-inquiry-into-youth-work-report-2019/

[28] Nearly 800 public libraries closed across Britain in the last ten years https://www.theguardian.com/books/2019/dec/06/britain-has-closed-almost-800-libraries-since-2010-figures-show See Research Library Briefing paper Number 5875, 20 June 2019 https://defenddigitalme.org/wp-content/uploads/2019/11/SN05875.pdf

[29] 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

[30] The CNIL deems facial recognition illegal at the entrance to high schools (October 2019) https://www.mediapart.fr/journal/france/281019/la-cnil-juge-illegale-la-reconnaissance-faciale-l-entree-des-lycees

[31] Sweden enforcement on facial recognition https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf

[32] "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/

[33] Stop posting children's faces online (2024) https://defenddigitalme.org/2024/01/28/call-on-the-education-sector-to-stop-posting-childrens-faces-online/

[34] Bessant, C. (2024) School social media use and its impact upon children's rights to privacy and autonomy | Northumbria University https://www.sciencedirect.com/science/article/pii/S2666557324000259

- **Introduce a ban on targeted advertising**, or using personal information to create profiles about school children or staff, selling or marketing their personal data, or onwardly disclosure to further third parties for purposes outside a school setting.
- **Ban upselling or 'in product' marketin**g in edTech including in-company or their affiliates.
- **End data brokers' routine access to school staff email** and intrusive, unsolicited marketing.

12. Security of data systems designed to protect children's digital footprint

- **Oppose any attempts to undermine encryption** and creation of "backdoors" into secure communications or edTech platforms, in order to protect public and personal data.
- Conduct education **sector audits for outdated infrastructure** (e.g. the "digital equivalent" of RAAC) that exposes the sector to malware, noting ever increasing cyber-threat and data theft.[35]
- 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 and standards in the digital environment

- **Introduce staff training on data protection and pupil privacy into initial 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 in line with domestic and all applicable data protection law[36] and guidance.[37]
- Ensure **ongoing training** is available and accessible to all staff for continuous professional development (CPD) for the delivery of quality education **in the digital environment.**
- Support at least the same level of understanding across school staff, as must be offered to pupils in 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).[38]
- **Clear and consistent human roles and responsibilities need definition.** The roles of school staff, parents/ families and children need boundaries drawn to clarify responsibilities and expectations around access to staff out of course, reach of cloud services into family and private life, including training on legal duties for digital monitoring in safeguarding children out-of-school-hours and in private time and spaces e.g. at home.
- **Employer and employee relations** need consistency and standards for the **management and ownership of digital materials and IP production in edTech products or controlled by educational settings (e.g recordings), worker surveillance, out of hours availability, responsibilities, and routes for redress when using automated marking and assessment**, and any algorithmic decision making with legal or other similarly significant effects.

14. Sustainable state education: infrastructure risk assessment and protection

- **Core national education infrastructure must be put on the national risk register**.[39]
- Key systems must have a **duty to national transparency reporting** obligations in order to understand their reach at scale and how much of the whole system is dependent on a few.
- **Ensure risk assessment is in place** for control of the core state education curriculum, staff training and quality, its delivery, threat management, data governance, and cost controls.

[35] Figures from the Information Commissioner's Office (ICO) show 347 cyber incidents were reported in the education and childcare sector in 2023 - an increase of 55% on 2022. In 2023 highly sensitive data was stolen from schools, including passport data https://www.bbc.co.uk/news/uk-england-gloucestershire-63637883 In Higher Education, UK Finance estimate that UK losses for the first half of 2018 due to cyber attacks were £145m. https://www.ncsc.gov.uk/report/the-cyber-threat- to-universities and poor practice can result in streaming or publication of data to people that should not see it https://www.blackpoolgazette.co.uk/education/parents-reassured-after-live-footage-from-blackpool-schools-cctv-cameras-was-hosted-on-us-website-342238

[36] Council of Europe Convention 108 Guidance for Data Protection in Educational Settings https://edoc.coe.int/en/children-and-the-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html

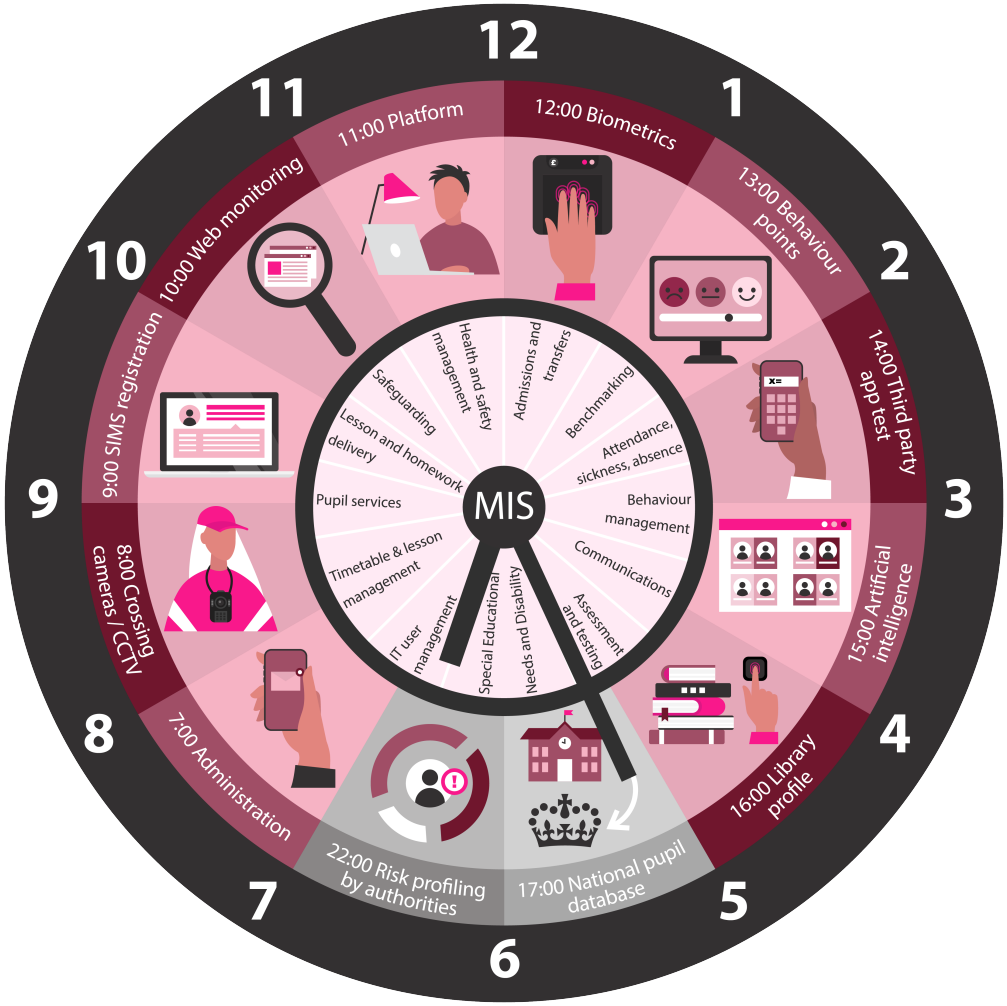
[37] ICO Codes of Practice https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/

[38] 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

[39] The National Risk Register https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf

How was your day?

Can you explain to a child and their family, where their digital footprint goes to from school on each and every day, and why?



About Defend Digital Me and what we do

Defend Digital Me is a call to action to protect children's right to privacy. We are a non-partisan, non-profit, civil society organisation. We campaign for safe, transparent and fair use of personal data across the education sector in England, and beyond. https://defenddigitalme.org/research/

@defenddigitalme | defenddigitalme.org | Registered at Companies House 11831192