DEFEND DIGITAL ME
BRIEFING- JULY 21, 2026

Twenty-one ministers, one children's data legacy

What each government built, what it cost children's rights, and what good looks like now

Reshuffles come and go. Since we began in 2014, we have seen a turnover of 21 Secretaries of State; ten in education and eleven in technology (split between DCMS and then DSIT). The data that we have worked towards making safe, fair and transparent for every learner in England outlives them all. Every child who started school in 2014 now has a decade-long record of named digital school records and its exhaust trailing behind them: 30 detailed census returns, assessment scores, safeguarding flags, EdTech logins, and a growing tangle of commercial and cross-government data-sharing they never agreed to and mostly can't see. We set this out in The State of Data 2020 full report, and little in the underlying architecture has changed since.

So when the ministers change again, it's worth asking each one a simple question. What was your digital policy, and did it add to or detract from children's rights?

> Every government of the last decade has expanded the collection, retention and commercial exposure of children's data at national scale faster than it has built the rights, transparency and redress to match. Children have lost control of their digital footprint by their fifth birthday simply by going to school.

These twenty-one ministerial legacies shape our landscape. The education-data that runs through the Department for Education embodied in the National Pupil Database, the school census, biometrics in schools, EdTech, and the safeguarding-monitoring estate. As of today, that responsibility now sits with Lucy Powell.

Their Venn diagram with tech, data-protection and children ran through DCMS, then DSIT — and, after this month's restructuring, splits again. This month's machinery-of-government changes broke DSIT up: online safety, digital identity, digital inclusion and "digital foundations" — along with the Government Digital Service and the Government Chief AI Officer — move into a strengthened **Department for Culture, Media and Sport** under Lisa Nandy; science, innovation, trade and AI adoption go to a renamed **Business, Innovation, Science and Trade** department under Jonathan Reynolds; and the AI Security Institute and a new AI Taskforce are pulled into the **Cabinet Office**, under Kanishka Narayan. Data-protection law, the age-assurance regime, the Online Safety Act and the ICO now sit largely with DCMS — and how all this dovetails with AI as an export and geopolitical power remains to be untangled.

All of these have intersections with Home Office policy that has spilled over from some of the same activity in their own domain: border control, immigration enforcement, and the DWP's fraud detection.

This is a mapping of where we understand so far, the Department for Education data and digital policy intersects with the machinery of government reorganisation of digital and tech policies and the continuing intersections of cross-cutting powers and interactions through national datasets.

What's next, and where might these Ministers take data and digital policy in state education?

Lucy Powell — Education (DfE)

Powell inherits the Act's implementation, the identifier build, the curriculum and assessment overhaul, SEND reform, and the unresolved EdTech data-selling scandal now under ICO audit. Crucially, she knows this terrain from the other side: as Shadow DCMS Secretary she shadowed the Online Safety Bill and the data-protection reforms. She arrives with an unusually strong grasp of the data-and-platforms landscape. What the Department has not yet done after the 2020 ICO audit (which should be published in full) must be done: put control over pupil data back in the hands of families.

Lisa Nandy — Culture, Media and Sport (DCMS)

Reappointed and handed a much-expanded brief, Nandy now holds the levers that matter most to children online. Under the July 2026 restructuring, DCMS takes on online harms, digital inclusion and skills, information resilience, the Government Digital Service (including GOV.UK One Login), the Government Chief AI Officer and the AI Incubator, and — moved from the Cabinet Office — responsibility for **digital identity policy**. That makes DCMS, not the old DSIT, the home of the age-assurance regime, the Online Safety Act's implementation and the under-16 social-media ban. Nandy's own background is in child welfare — Centrepoint and The Children's Society — which is exactly the lens this brief needs, if the department can resist the drift from protecting children to identifying everyone.

Jonathan Reynolds — Business, Innovation, Science & Trade (DBIST)

Reynolds leads the renamed business-and-trade department, taking on science, innovation and — critically — AI *adoption* and frontier technology. That framing structurally privileges growth and commercial application over rights. He still shapes the Data (Use and Access) Act's automated-decision provisions, the science-and-data commercialisation agenda, and the reuse of pupil data for research and product development. His background is business and trade, not digital rights. That sets the tone of the challenge.

Kanishka Narayan — AI safety, at the Cabinet Office

The AI Security Institute and a new AI Taskforce in the Office for the Prime Minister sit with Narayan at the centre of government. But note what this leaves: the person titled Chief AI Officer now sits in DCMS, AI *adoption* sits in DBIST, and AI *safety* sits in the Cabinet Office. There is a Chief AI Officer who does not own adoption, an adoption drive with no chief, and a safety institute walled off from both. For children's data — which flows into all three — there is no obvious single accountable owner, and no clear collaborative goals in their overlap.

> AI touching children's data now has three homes across government and no single owner: the Chief AI Officer in one department, adoption in another, safety in a third. Fragmented accountability is how respect for rights and meaningful responsibility fall through the cracks.

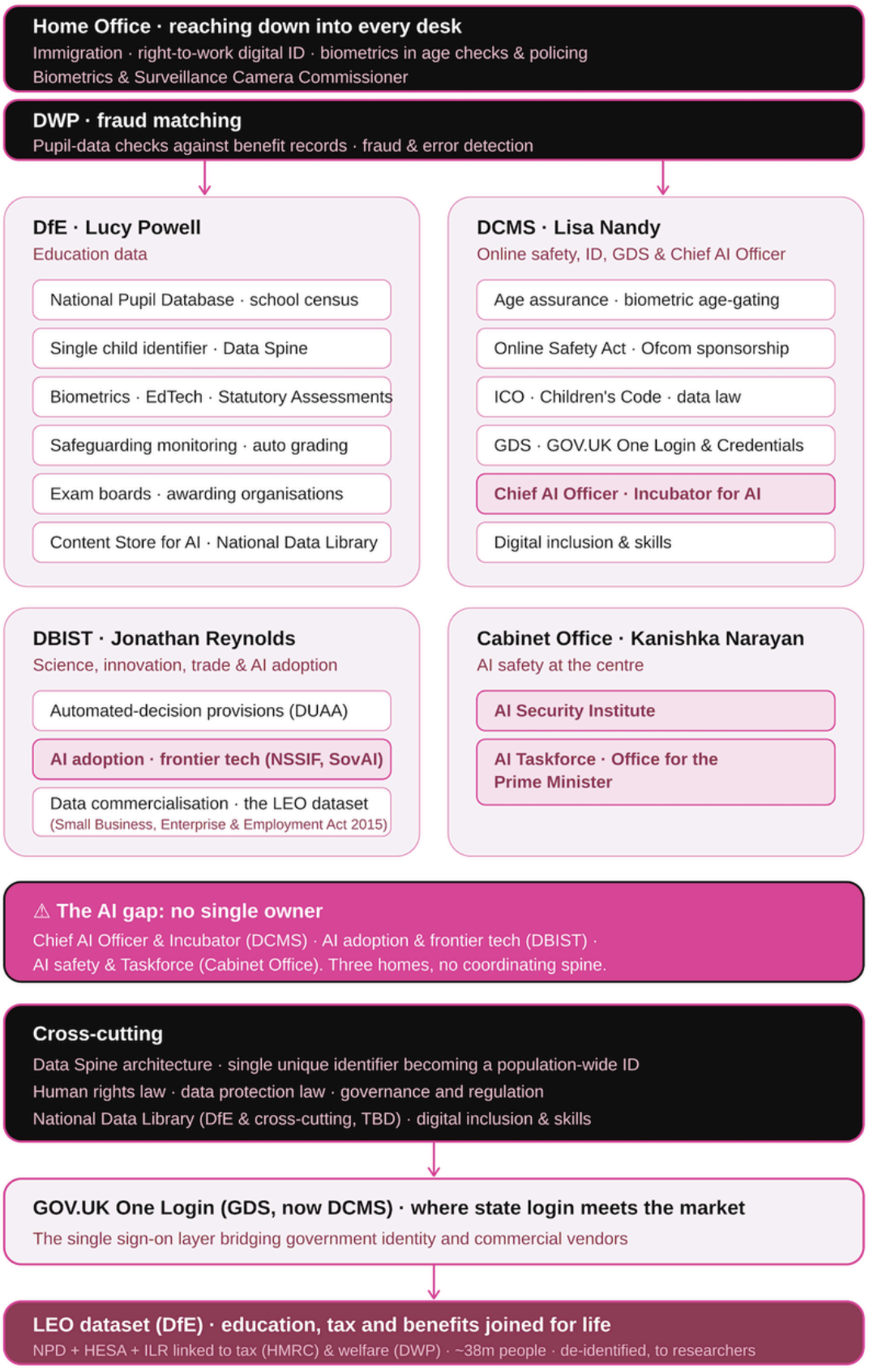
Mission and vision are missing any clear strategy

Ten education secretaries. Eleven holders of the tech and data brief. We have now outlasted them all, but the underlying mission and vision has not had clear strategy in either domain, or across both where they overlap, except in AI.

1. **Collection has consistently outrun rights.** Every flagship measure added data faster than it added transparency, consent or redress.
2. **Scope creep is the norm.** Data collected for one purpose reliably ends up serving another.
3. **The genuine wins are rights-by-design.** The nationality-data climbdown protected children by removing data exposure and upholding their rights and freedoms.
4. **Ministerial churn is a children's-rights risk.** Institutions, not ministers, must carry the safeguards.

> For a decade, every minister has expanded children's data use more than they have protected it. The single child identifiers and the age-assurance regime are the two levers that will define the next decade. Built within a human rights framework for the person the system is about, you might build trustworthy participatory systems. Built for the state and for authorities' control and intervention, you build national surveillance from childhood that lasts a lifetime.

Where new ministerial responsibilities map into education data and digital policy



*Our understanding on July 21, 2026 from information available in the public domain, subject to change

Two futures for children's data and digital lives coming through education

Underneath every one of these flagship policies sits a choice between two futures — and it is not only ours to describe. When we asked young people directly, in the workshop behind The Words We Use in Data Policy (2021), they named both futures for themselves.

Seeing like the State: is data as, in the government's own repeated phrase, *fuel for the economy* — or as one former Culture Secretary put it plainly, *"data is oil."* It runs on collection: a linked-up Data Spine, a single lifelong identifier, a plan to "mainline AI into the veins" of public services. In this vision the National Pupil Database is infrastructure to be expanded, the research justification quietly slides into operational and punitive reuse, and children are turned, in our report's words, into product to *"mine, extract and exploit and pass around to others."* It is the vision in which a Labour promise made in 2002 — that pupil names were for statistics only — became meaningless, without a single vote in Parliament, a monthly feed to the Home Office and the police. The young people we worked with recognised it at once: data as something that, as one put it, *"follows you around from even before you are born and… can dictate how people deal with and treat you."*

> Policemen will just rely on data — like name, date, binary information — but I have my own truths. Nothing and no one can tell me what I am.
>
> — ALEX, AGED 14–21, THE WARREN YOUTH PROJECT

That first model, the report concludes, *"will fail. Young people do not support it and even take action to resist and refuse such collections."* The nationality-data boycott and the care.data collapse are what happens when the State collects without a social licence.

Ours is safe, fair and transparent data: a landscape that, again in young people's own words, *"supports data access not distribution, in which they have controls over its use with respect for their life stories."* We mapped how to get there in The State of Data 2020 — every flow of children's data in, across and out of state education — and set out the legislative route in our manifesto for an Education and Digital Rights Act. The principles are simple and long-established in law: children and families are told the data exists and can exercise their rights across the full life cycle; identifying data is not retained forever "just in case"; genuine public-interest research is served by safe access, not by handing out copies; and the child's right to education comes before commercial or operational reuse. As we put it in the report: there is *fairness, not ownership.*

Above all there is no joined-up vision for the future of society underpinned by digital citizenship skills for every segment of the population, for every age group.

> We are "more than a score." Data cannot contain the complexity and fullness of a human life — and the systems built on it look only backwards, at what was, not is.

The single child identifier and the age-assurance regime are where these two visions now collide. Every ask below, is an attempt to make the second vision — the one children themselves ask for — win on purpose, rather than let the first win by default.

The DfE Data Spine, a chance now to not repeat past mistakes

The clearest place these two visions meet is the DfE's planned Data Spine and the single child identifier likely to be built on the NHS number. Because it is new, it is the one chance in a generation to build a national children's data system that gets it right from the start — or to hard-wire in the failures we already know.

Those failures have names. The NHS's care.data collapsed under mass opt-outs when the public discovered data was being moved without a social licence. The DfE–Home Office data-sharing turned education records into an immigration-enforcement tool. Both share the same design faults the Data Spine must not inherit:

- **Centralisation without consent** linked stores of everything, built without telling the families in it.
- **Opaque infrastructure** —increasingly run on U.S.-owned platforms (AWS, Palantir, Databricks) whose data flows the public cannot see or audit.
- **Data about us, without us** — no fair processing, no meaningful way to be informed, object or opt out, in breach of the very GDPR articles the ICO's own 2020 DfE audit already found the Department failings that are yet to be fixed, six years on.
- **Scope creep by default** — a single unique identifier for "safeguarding" purposes for a few, can quietly become a cross-government linkage key for welfare, immigration and policing for everyone.

Repeat those, and the result is predictable: a catastrophic loss of public trust, mass opt-outs, and a database too mistrusted to serve even the research and safeguarding purposes it was built for. Build a new spine on the old faults and it fails the same way — only bigger.

> There is a sense of big brother about it all. Infant school, they've got your whole life in a data bank — how is that information going to be utilised?
>
> — PARENT OF A GCSE PUPIL, DFE / DSIT PUBLIC ATTITUDES RESEARCH, 2024

This isn't guesswork — it's what parents told the government they want.

The DfE and DSIT's own 2024 deliberative research on public attitudes to AI in education asked parents and pupils directly. Their answers are a design brief for doing it right — and a stark warning against the current direction of travel:

- **Tell us, and ask us.** There was, in the researchers' words, widespread consensus that work and data should not be used without parents' and pupils' explicit agreement — with clear information about why data is collected, who can access it, and how long it is kept.
- **No identifying data.** Participants felt strongly that personally identifiable data such as name and date of birth should not be re-used at all — it was seen as unnecessary and too risky when linked with other records.
- **Keep identifiers at school level.** Parents and pupils said that where data is pseudonymised, identifiers should be held at school level and not shared with tech companies or central government.

- **No SEND data sharing across departments.** Parents of children with SEND were especially clear: they did not want their child's SEND status shared between government departments, fearing it could affect benefits, university, or future employment.
- **Distrust of central databases and tech companies.** Many worried about surveillance if most of the population's data ends up held and used by a limited number of central organisations, and trust in tech companies to protect data was, in the report's words, extremely limited.

Every one of those findings maps onto a design choice the Data Spine has not yet made. The public has already written the specification. The only question is whether the next ministers build it.

What good looks like in 10 years time: our vision for what's possible

Ten years from now, good looks like a data policy and practice framework that treats the whole arc from birth to 25 as one coherent duty rather than a series of disconnected consent moments. A child's record — created from data collected in attainment tests and school censuses, some of it added from before birth and kept for a lifetime — is governed by clear lawful bases, strict purpose limitation, and enforceable minimisation, with sampled and aggregated data replacing the wholesale retention of named pupil records at national level. Every young person, and their parents where appropriate, can see their own school record through a simple access route and specify how it is managed — what is held, who it is shared with, for what purpose, and for how long — reflecting DDM's proposed parental-controls model and what parents and pupils asked for in the DfE/DSIT research: that pseudonymised identifiers stay at school level and aren't shared with tech companies or government. Sensitive data — SEN, free-school-meals status, ethnicity, health flags — is a deliberate step-up choice, never a hidden default; the default is that the system collects as little as it can, not as much as it might, and that no choice a family makes is ever punitive.

Good also looks like access to public services supported by data, not driven by it — systems that serve the public rather than being powered by its personal data. Children and families use education, health, and welfare services without their records being quietly repurposed: the Home Office matching of pupil records for immigration purposes, and the use of the National Pupil Database for DWP fraud and criminal investigations, ends. The department that holds a nation's data is no longer the Big Brother of that nation, but its respected older uncle — the one who looks out for us, not at us. National surveillance infrastructure is replaced by trustworthy systems that earn and encourage trusting interaction, built on the foundations DDM set out in The State of Data 2020, whose recommendations span ten areas:

1. Legislation and statutory duties
2. Assessment, attainment, accountability and profiling
3. Administrative data collections and national datasets
4. Principles and practice using technology today
5. EdTech evidence, efficacy, and export intentions
6. Children's rights in a digital environment
7. Local data processing
8. Higher Education
9. Research
10. Enforcement

Together they point to a statutory Education and Digital Rights Act, independent oversight through a national guardian, and a genuine social licence rooted in what children and families actually want. People engage more openly, and public services work better, when the relationship is one of care rather than watchfulness.

That framework rests on digital infrastructure built to be rights-respecting by design: interoperable, transparent, and accountable, with data-minimising methods — cryptographic age assurance and zero-knowledge proofs — replacing the wholesale capture of faces and identity documents. On that foundation, the online experience becomes one where protection, privacy, and participation reinforce rather than compete. Children can access, explore, and take part in digital life without trading away their identity; safety is achieved without turning every service into a gate that excludes or a mechanism that profiles. The measure of success is a settled default in which a young person's best interests — their right to privacy, to access, and to participation — are served reliably, and no longer depend on the commercial or regulatory convenience of everyone else.

Background lessons to avoid and to learn from

The threat model: how a children's database becomes everyone's ID

To see why the architecture matters more than any single policy, follow where the pipes already run. Education records are not a closed system. Through the same linkage infrastructure, pupil data has reached the **Home Office** for immigration enforcement — the DfE–Home Office data-sharing deal that turned school registers into a tracing tool — and, as our own casework revealed, the **Department for Work and Pensions**. Under a data-sharing arrangement formalised in autumn 2023, DWP fraud investigators have been able to check individuals against the National Pupil Database; DWP had been requesting pupil-data matches since 2018, framed as confirming the "right amount of benefit" and enabling the department to "identify and prevent fraud and error" and pursue overpayments. School leaders warned it risked families withdrawing children from school altogether. As we said at the time, pupil data should be used for the purposes of a child's education and that alone — not for the DWP to hunt people down. The direction of travel is always the same: a dataset gathered to help a child is quietly repurposed to police a household.

Now watch that same architecture surface at the other end of life. The government's digital ID scheme was launched in September 2025 to prove the **right to work**. After a petition of nearly three million signatures, ministers dropped the word "mandatory" for the ID card itself in January 2026 and something still to be described was scrapped this week — but kept digital right-to-work checks mandatory and still intend full digital checks by the end of this Parliament. The label softened; the architecture and the intent have not. Scope creep does not need a card to be compulsory. It only needs the underlying plumbing to exist and that's not going anywhere, even if the policy is 'scrapped' on media and news headlines.

The plumbing is being laid increasingly in children's lives. To enforce the under-16 social media ban, platforms must now verify every user's age: ID or a face scan before you can open an account. To run the July 2026 overnight curfew for 16- and 17-year-olds, the system must do something even more precise — tell a 15-year-old from a 16-year-old from a 17-year-old, and switch features off by the hour. Add the proposed **gaming restrictions and curfews**, and you have built, in the name of protecting children, a nation-wide apparatus for continuously proving exactly who and how old everyone is. To age-gate the internet for children, you have to identity-gate it for adults too.

> To tell a child of different ages apart from an adult, the system has to check everyone. The age-gate built for children is an identity-gate for the whole population — and the Home Office has found its way in through the nursery door. That's not to underplay the seriousness of child protection but it demands an understanding of how these contests for power and competing aims interplay.

The Home Office still drives so much of what it does through the lens of the Hostile Environment. It began as a policy aimed at a minority; it is becoming an infrastructure that touches everyone, reaching — like an underground network running beneath the ordinary world — into work, welfare, play and speech. The Home Office has found a way into all our lives, and it found it through children. Our own analysis has warned that mandatory age verification will not even deliver the child protection promised, while excluding vulnerable groups and normalising the very identity checks it claims are exceptional.

And whoever builds the plumbing controls the flow. The systems that would hold, match and verify all of this identity data are not sovereign public infrastructure — they run increasingly on **U.S.-owned platforms: Palantir, Databricks, AWS, Google Cloud** and their peers. The age verification providers' layer sits on top of the civil identity data held by the state and by commercial firms. A decision to age-gate British childhood becomes, at the infrastructure layer, a decision to route the identity records of the entire population through a handful of commercial giants, under legal regimes and commercial incentives no parent ever agreed to or can even see behind the screen.

In Education, this is the real stake in getting the DfE Data Spine right or wrong, safe, fair and transparent. It is not the glue between children's databases in education, health and children's social care. It is the gatekeeper for how everyone in England, minus the 7% in private education, will be known to the state.

The National Pupil Database: what DfE got wrong and still needs to fix

28m+
people's records held in the National Pupil Database — everyone in state education in England since 2002

2,385*
separate bulk distributions of identifying, sensitive pupil data to third parties since 2012

39%
of legacy NPD requests were tier 1 — the most identifying and highly sensitive category

2,136
one school's pupil records handed to Merseyside Police in a single request — 97% of the entire 10-year police total

28m
learner records exposed when Trustopia used its database access to give age-verification company GBG for gambling clients' onboarding

10
education secretaries since 2014 — no sustained ownership of children's data policy

*Each of those 2,385 distributions was a bulk batch — a single release may contain thousands or millions of individual identifying longitudinal records, not only one person's file. When last asked, the Department did not track how many individuals' data was in each release. Figures from our 2026 review of national pupil data distribution; full dataset and workings published there.

Ten asks for Lucy Powell at Education to fix where we are now

The framing: the single child identifier and the Children's Wellbeing and Schools Act make this the most consequential moment for pupil-data rights in a generation. Ship it with rights, or ship Database State 2.0. The ten asks below distil our key proposals, set out in full in our manifesto for an Education and Digital Rights Act and our practical model in Pupil data: respecting rights for EdTech and the NPD.

1. **Rights-by-design for the single child identifier** — hard purpose-limitation, a public register of every data use, identifiers held at school level, and a child- and parent-facing access-and-objection mechanism, legislated *before* it goes live. Build the Data Spine to the public's own specification, not around it. Make rights something parents and learners can see and realise in real experience, not read on paper.
2. **A statutory transparency duty over the National Pupil Database** reuses— every third-party access published proactively, and a personal record of use available to every pupil and parent.
3. **A purpose-limitation lock on cross-departmental sharing**, in line with what parents told you they want — a statutory bar on education data, and SEND data in particular, flowing to immigration enforcement, welfare or policing.
4. **An independent review of Reception Baseline and all statutory assessment data retention** — justify lifelong retention against a benefit-to-the-child test, or stop. End the context collapse of wider reuse at LA level for all sorts of purposes that the data were not designed for.
5. **Automated-decision and profiling rights in education** — a right to human review and required communication of any automated decision about a learner.
6. **A data-governance capacity floor for all admin data in educational settings** — minimum standards as a condition of trusted status must be informed by a statutory data protection Code of Practice for educational settings, informed by our State of Data 2020 findings and ICO audit.
7. **Data-rights, digital-skills and AI literacy — start in teacher training** — grounded in the Council of Europe's digital citizenship education and AI-literacy framing (critical, rights-based citizenship, *not* business "how to use the tools for 'efficiency'"). Today there is effectively nothing on data rights or AI literacy in initial teacher training; make it a core strand of ITT so every new teacher can teach it, then extend a genuine AI-literacy entitlement across the whole population — children, parents and the wider public — not just the workforce.
8. **Review the Data Spine architecture and first sunset and minimise legacy census fields** — retire anything without a current, lawful, child-benefiting purpose.
9. **Build continuity of accountable ownership** — a permanent senior data-rights lead, so churn stops resetting the safeguards. Build a National Data Guardian like health already has.
10. **A children's-data floor for EdTech procurement** — extend the Chartered College's EdTech Evidence Board beyond effectiveness to a binding no-commercial-reuse data standard.

Eight asks for Lisa Nandy at Culture, Media and Sport: to fix where we are now

With online safety, age assurance, digital identity, GDS and the Chief AI Officer now housed at DCMS, this is where the age-gating agenda will be won or lost. Housing these levers alongside "digital foundations" and a growth-focused digital-inclusion brief risks treating children's rights as friction. The ask is to prove that framing wrong — and to use a child-welfare background to hold the line between protecting children and identifying everyone.

1. **Uncouple "child safety online" from "universal age verification"** — an honest technical and rights assessment, starting from the "VPNs are out of scope" learnings. Scrap the curfews plan, as they do not work.
2. **No mandatory facial age estimation without a proven, less-intrusive alternative** — data-minimising age assurance, not the biometric mass-processing of children's faces.
3. **Reinstate the automated-decision protections weakened by the [Data (Use and Access) Act 2025](https://www.legislation.gov.uk/ukpga/2025/18/contents)** — restore the meaningful right to human review. Reinstate the balancing test for new conditions of legitimate interests.
4. **A genuinely independent data regulator** — protect ICO independence, reputation, and enforcement capacity against pro-innovation pressure.
5. **Extend, don't dilute, the Children's Code** but bring it back to its core ICO remit, data not "safety" — bring AI companions and generative tools explicitly within scope.
6. **A children's-rights impact requirement for AI governance** — aligned with UNCRC General Comment 25. With the Chief AI Officer now at DCMS but AI adoption at DBIST and AI safety at the Cabinet Office, this cannot be left to fall between the three.
7. **Corporate accountability with teeth** — turn the 28-company ICO audit into a durable AI enforcement regime that goes beyond data.
8. **Resist the deregulatory ratchet** — a public commitment that no future data bill trades the human rights of everyone for 'innovation', i.e. company profit for a few.

And for Jonathan Reynolds at DBIST and Kanishka Narayan at the Cabinet Office: with science, innovation, data-commercialisation and AI adoption now under DBIST, hold the line that children's data is not an economic input to be traded for growth — starting with the Data (Use and Access) Act's automated-decision provisions and any science-and-research reuse of the National Pupil Database. And with the AI Security Institute and AI Taskforce now at the centre of government, a children's-rights impact requirement for public-sector AI, aligned with UNCRC General Comment 25, belongs at the heart of the AI agenda — not lost between the three departments that now share it.

The history of how we got here

Part one: education-data and the DfE

What each minister built, and what it cost children's rights

Michael Gove (to July 2014)

Gove's "opening up" of the National Pupil Database to bulk third-party access — researchers, journalists, commercial re-users — handing out individual-level pupil records with no pupil or parental knowledge or consent, was botched from day one. Every problem since is a variation on the transparency and consent deficits that were created, which we mapped in full in The State of Data 2020 full report.

Nicky Morgan (2014–2016)

The 2016 addition of nationality and country-of-birth fields to the pupil census triggered our first national campaign. Those fields, later shown to be intended for immigration-enforcement data-sharing, proved our central argument: education data is never *just* education data. The fields were suspended in 2018 after sustained pressure but when Nick Gibb (July 2016, PQ 42842) denied plans to share the nationality data — the DfE–Home Office monthly data-sharing had already been live since July 2015, under an MoU predating his denial. Between July 2015–September 2016: Home Office made requests on 2,462 individuals, DfE returned 520 records (PQ 48635, Oct 2016). The 2016–18 nationality/country-of-birth data was deleted in 2021 after the ICO audit — but the monthly Home Office handovers of other pupil data continued.

Justine Greening (2016–2018)

Greening's tenure is our textbook case of function creep. The DfE–Home Office data-sharing Memorandum of Understanding — pupil records used to trace immigration status — is the reason "purpose limitation" is in every submission we write. The full sequence of complaints, the ICO's compulsory audit and what followed is set out in our National Pupil Data and ICO audit timeline.

> Education data reached the Home Office. "Online safety" became universal age-verification. A "single identifier" for safeguarding is a linkage engine for everything else. Function creep is the norm, not the exception.

Damian Hinds (2018–2019)

Hinds' 2019 EdTech Strategy marked the pivot from *government* data collection to *commercial* data extraction as the growth frontier — with no matching data-protection floor. It is the direct policy ancestor of the 2026 revelation that an EdTech firm sold children's profiles — and of the earlier Learner Records Service breach, where Trustopia used its access to give gambling companies age-verification data on 28 million learners. We said that was structural, not accidental. The DfE's own answer in the form of the Chartered College of Teaching's EdTech Evidence Board assesses products for educational *effectiveness*, but not yet against a binding children's-data-protection floor. That gap is where the harm comes from.

Gavin Williamson (2019–2021)

The 2020 "mutant algorithm" exam fiasco is the most vivid public demonstration of everything we say about automated decisions on exams and how to fix them. An opaque model assigned life-altering grades, hit disadvantaged pupils hardest, and offered no meaningful appeal. It was the moment automated decision-making in education became a doorstep issue.

Nadhim Zahawi (2021–2022) et al.

Zahawi's academy-trust build-out concentrated data controllership in Multi-Academy Trusts with wildly variable governance capacity — a structural risk we hit repeatedly in our State of Biometrics 2022 review. Michelle Donelan's two days and Kit Malthouse's brief tenure added nothing lasting, but they make a different point: ten education secretaries since 2014 means no sustained ministerial ownership of children's data. Churn is itself a risk.

Gillian Keegan (2022–2024)

The Reception Baseline Assessment epitomises "collect first, justify later" — testing four-year-olds and folding the results into a lifelong record, with no demonstrated benefit to the child.

Bridget Phillipson (2024–2026)

The most significant — and most double-edged — development in a decade. The Children's Wellbeing and Schools Act and the single "consistent child identifier" across education, health and social care is exactly the data-linkage infrastructure we have long warned about: huge potential for safeguarding benefit *and* for profiling, surveillance and function creep. Whether it ships with rights, transparency and hard purpose-limitation — or as Database State 2.0 — is the open question handed to her successor. Our 2026 review of national pupil data distribution sets out the scale of what already exists: the National Pupil Database now holds data on **more than 28 million people** — anyone who has been in state education in England since 2002 — and identifying, sensitive pupil records have been handed to third parties in at least **2,385 separate bulk distributions since 2012**, each release potentially covering thousands or millions of individual longitudinal records. The single question that has to be answered before anything is built on top: is the NPD a research database, or an operational one? It cannot lawfully be both.

> Either you can have a research database and enjoy its research exemptions, *or* it can be operational and must support people's rights. The Department cannot lawfully have its cake and eat it.

The promise it started from is worth remembering. When names were first added to the database, the then minister Stephen Timms told Parliament in 2002 that the Department had *"no interest in the identity of individual pupils as such"* and would use the data *"solely for statistical purposes."* Two decades later, records flow monthly to the Home Office, police and courts, and your unique pupil number — like your NHS number — stays with you for life.

The identifying data given out in these releases is not limited to names and addresses: it includes the results of statutory assessment — Key Stage tests, commonly known as SATs — attached to identifiable pupils, retained and re-shared for life. How often each category of data has been released is, in principle, visible in the DfE's own published external data shares tables, and in the full dataset we cleaned and merged for the 2026 review — though the DfE has never itself published a plain summary of how many individuals, or which fields, sit inside each bulk release.

Our proposed way through — a rights-respecting model for EdTech and the National Pupil Database — is set out in full in Pupil data: respecting rights for EdTech and the National Pupil Database.

Part two: the tech and data-protection pathway (DCMS, DSIT and BIST)

John Whittingdale (2015–2016) laid the groundwork for the Digital Economy Act 2017's age-verification regime for online pornography — a scheme eventually abandoned as unworkable and privacy-hostile. Those exact failure modes — identity honeypots, exclusion, mission creep — are what we now cite against the 2026 age-gating proposals.

Karen Bradley and Matt Hancock (2016–2018) delivered the Data Protection Act 2018 and UK GDPR — foundational to all our casework — but baked in a digital age of consent of 13 and a weak enforcement culture we still work to fix. Hancock also championed what became the Age Appropriate Design Code, the subject of our own report, The Best Interests of the Child and the Age Appropriate Design Code.

Jeremy Wright (2018–2019) published the Online Harms White Paper, launching the online-safety regime. Our position from the start: safety and privacy are not opposites, and a duty of care built on age-assurance and monitoring risks mandating the surveillance of childhood in the name of protecting it.

Nicky Morgan (2019–2020) — yes, the same Nicky Morgan, now on the tech side, oversaw early progress on the Children's Code, which came into force in 2021.

Oliver Dowden (2020–2021) launched the post-Brexit "Data: a new direction" agenda, reframing data protection as red tape. We frame it as children's rights infrastructure — the argument we made in The Words We Use in Data Policy runs through the entire second half of the decade.

Nadine Dorries (2021–2022) drove the Online Safety Bill through its most contentious phase while championing the original Data Protection and Digital Information Bill, the biggest deregulatory threat to children's data rights in years, weakening subject access, automated-decision protections and independent oversight. Most of it came back again later.

Michelle Donelan (2022–2024) split "Digital" out to create DSIT, passed the Online Safety Act 2023, and relaunched the data bill. The OSA hard-wired age assurance into law — the mechanism now driving the facial-age-estimation and "liveness checks" rollout we are actively rebutting. This is where "protect children online" became "verify everyone's age": the conflation we exist to challenge.

Peter Kyle (2024–2025) passed the Data (Use and Access) Act 2025 — Labour's successor to DPDI, reviving many of its provisions — and pushed the OSA implementation and Ofcom age-check codes that put mandatory age checks and the under-16 social-media-ban debate on the front pages.

Liz Kendall (2025–2026) carried the social-media minimum-age proposals and the age-assurance rollout, although we welcome the news that VPNs are "out of scope". The ICO audit finding EdTech-profiles-sold scandal and the ICO's audit of 28 companies also broke on her watch but there was nothing mentioned to parliament or efforts to coordinate the news with the DfE and take action to support schools in better procurement choices, vindicating our corporate-accountability line and call for action since 2017 on the need for an enforceable data protection code of practice in education. This needs to happen now.

Our key proposals & solutions

- **Manifesto for an Education and Digital Rights Act (2024)]** https://defenddigitalme.org/wp-content/uploads/2024/06/Defend-Digital-Me-manifesto-2024-v2.0-1.pdf — our core proposals
- **Pupil data: respecting rights for EdTech and the National Pupil Database (2026)]** https://defenddigitalme.org/2026/04/29/pupil-data-respecting-rights-for-edtech-and-the-national-pupil-database/ — our key solution
- National pupil data distribution: a 2026 review, and how to fix it — with the DfE's own external data shares tables

The casework & the ICO audit

- National Pupil Data, the ICO audit, and our work for change: a timeline
- The Learner Records Service data breach and ICO audit: a connected chronology (Trustopia / 28m records)
- EdTech firm sold children's profiles — ICO audits 28 companies (2026)
- Schools Week: the secret DfE–DWP deal letting the benefit-fraud squad check pupil data (2024)

Our research referenced here

- The State of Data 2020 full report · overview · The State of Data 2018
- The State of Biometrics 2022
- The Words We Use in Data Policy (2021)
- The Best Interests of the Child and the Age Appropriate Design Code (2021)
- The Under-16s Social Media Ban FAQ · Age-gating the internet
- Government evidence: DfE / DSIT research on public attitudes to AI in education (2024) — what parents and pupils said they want

Key legislation & standards

- Children's Wellbeing and Schools Act · Data (Use and Access) Act 2025 · Online Safety Act 2023
- Data Protection Act 2018 · Digital Economy Act 2017
- UNCRC General Comment No. 25 · Chartered College EdTech Evidence Board

---