5RIGHTS
FOUNDATION

The Data (Use and Access Bill) and children's data

House of Commons, Committee Stage Evidence
5Rights Foundation
March 2025

Summary

- The Government's Data (Use and Access) Bill will introduce a number of changes to the UK's data protection framework (UK GDPR) which will impact children's privacy and safety.
- It is vital that changes to UK GDPR do not water down existing protections for children, including the Age Appropriate Design Code which sets out the standards for the use of children's personal data.
- Changes made to the bill during the House of Lords stages are welcome, but clarity and timelines are still required on:
- Changes to automated decision making in particularly leave children particularly vulnerable. The Government must bring forward a code of practice on AI and automated decision-making as soon as possible to establish guardrails that will keep children safe.
- The Government must maintain amendments made in the House of Lords to narrow the scope in which children's data can be used for scientific purposes. Children's data must not be allowed to be misused for the commercial interests of tech companies, including and in particular AI developers.
- New legal duties in GDPR to give children data protection by design and default must be recognised and enforced by the Information Commissioner's Office. This is crucial to realising children's rights and needs in the digital world, protecting their privacy and keeping them safe.
- The Government must bring forward its promised code of EdTech as soon as possible, owing to the vastly unregulated nature of this sector and the repeated malpractice of children's data by EdTech companies.
- Children's intellectual property must be safeguarded, and the Government must rethink its proposals to prevent an AI 'free for all' on children's protected works. This is crucial in school environments, where children should be shielded from all forms harm – including economic and commercial exploitation.

Introduction

The over-use of children's data increases their risk of harm. It is used to power toxic algorithms that trap them in cycles of harmful content,[1] recommender systems which connect them with predators[2] and discriminatory AI systems used to make decisions about them with life-long consequences.[3] Children are uniquely vulnerable when their data is not handled in their best interests – giving them a high level of data protection is fundamental to keeping them safe and is central to upholding their rights online.

The UK is a world leader on children's data protection. In 2018, Parliament introduced the **Age Appropriate Design Code**[4] as part of the Data Protection Act, which set out 15 standards organisations must abide by when handling children's data, enforceable by the Information Commissioner's Office (ICO). Since it came into force in 2021, companies around the world – including the biggest tech companies in Silicon Valley – have made changes to the design of their platforms in order to make them safer for children.[5]

We welcome concessions made during the Bill's passage through the House of Lords that seek to embolden the existing standards of heightened protection for children. It is crucial that the Government remains committed to protecting children's privacy – particularly as it is inextricably linked with children's safety in the online world.

Any proposals by Government to make changes to the UK's data protection regime must uphold these vital protections that keep children safe and protect them from harm.

At a glance: Implications of the Data (Use and Access) Bill

5Rights welcomes provisions in the Bill which will increase accountability of tech platforms. The bill will amend the Online Safety Act to allow **researchers to access data from social media companies** to develop understanding of how the design of their platforms cause harm, building on measures that give **coroners access to data** to support inquests into the deaths of children by putting in place data preservation orders. These provisions will ensure that tech companies are held accountable for harms to children on their services.

However, certain provisions in the bill which will amend key principles of the UK's data protection regime (UK GDPR) risk watering down existing protections and transparency requirements on children's personal data and will expose them to harm. The Secretary of State for Science, Innovation and Technology has stated that he wants to see an online

[1] The inquest into the death of 14-year-old Molly Russell found that she "died from an act of self-harm whilst suffering from depression and the negative effects of on-line content." See: *Molly Russell: Prevention of future deaths report*

[2] See: The Verge (2023) *Instagram's recommendation algorithms are promoting paedophile networks*

[3] Eynon, R. (2023) "Algorithmic bias and discrimination through digitalisation in education: A socio-technical view." *World Yearbook of Education 2024*

[4] 5Rights Foundation (2021) *UK Age Appropriate Design Code*

[5] See: Woods, S. (2024) *Impact of digital regulation on children's digital lives*, Digital Futures for Children Centre, 5Rights Foundation, London School of Economics

world with children's safety "baked in from the outset."[6] Protecting children's data against misuse must be a core part of achieving this aim.

We welcome many of the changes made in the House of Lords, which seek to remedy several of the issues with the Government's approach on safeguarding children's data. However, greater clarity is still needed in certain areas.

1. Safeguarding children and their data within automated decision-making, AI and machine learning

Clause 80 (Automated decision-making) of the Bill would change Article 22 of UK GDPR[7] from a general prohibition on the sole use of automated decision-making (ADM) without human involvement in decisions with a legal or similarly significant effect to *only* being prohibited if based on special category data.

The impact assessment for the Bill makes clear that one of its aims is to support the use of data for AI and machine learning.[8] However, whilst the Bill brings forward new safeguards that prohibits ADM based on special category data, and ensures data subjects must be informed where this happens and allows them to request human oversight, this will not mitigate the risks of unfair and discriminatory decisions which are still found widely in AI systems. The impact of these erroneous decisions are felt most acutely by children and other vulnerable groups.[9][10][11]

Removing special category data will not prevent discrimination

Removing special category data from ADM does not prevent discriminatory outcomes as many AI models can learn bias based not on protected characteristics, but by other features closely correlated to these characteristics.[12] For example, a model that does not include racial background but does include surnames can be used to infer this background.

Case study

[6] Department for Science, Innovation & Technology (2024) *First UK-US online safety agreement pledges closer co-operation to keep children safe online*

[7] Information Commissioner's Office (ND) *What does UK GDPR say about automated decision-making and profiling?*

[8] Department for Science, Innovation & Technology (2024) *Impact Assessment for the Data (Use and Access) Bill*, p. 2

[9] AI tools used by the Home Office have the potential to "encode justices" and automate the approval of life-changing decisions. See: The Guardian (2024) *'AI' tool could influence Home Office immigration decisions, critics say*

[10] In 2020, 39.1% of pupils A-Level grades in England were downgraded as a result of a 'mutant' algorithm used to predict their results. The algorithm in particular favoured private schools and impacted disadvantaged areas the hardest. See: The Guardian (2020) *A-Level and GCSE results in England to be based on teacher assessments in U-turn* and *England A-level downgrade hit pupils from disadvantaged areas hardest*

[11] Research into machine-learning models in the social care system found that, on average, if the model identifies a child at risk, it is wrong 6 out of 10 times. Further, machine-learning models missed 4 out of 5 children at risk. See: What Works for Children's Social Care (2020) *Machine learning in children's services: Does it work?*

[12] AI Blindspot (ND) *Discrimination by Proxy*

> An algorithm used in a school safeguarding software which refers children to the Prevent programme replicates historic biases against children from minority ethnic backgrounds. Removing ethnicity as a feature would not remove the bias – we would still expect the model to disproportionately over-flag children with surnames suggesting a certain ethnicity.

This issue has been raised previously by the ICO,[13] who has said that "*simply removing special category data (or protected characteristics) does not guarantee that other proxy variables cannot essentially reproduce previous patterns… These problems can occur in any statistical model, so the following considerations may apply to you even if you don't consider your statistical models to be 'AI'.*" Biases can also be unintentionally embedded by developers too, for example in the qualities of the best candidate for a job.[14]

The right to contest these decisions is not a sufficient safeguard

Research suggests that humans tend to defer to decisions made by algorithms, especially where the decision is a difficult one.[15] The right to contest decisions made by ADMs which is included in these changes is welcome but is not a sufficient safeguard.

Safeguards to ensure data subjects are aware of decisions made by using solely ADM may not deliver transparency

5Rights and ICO research has demonstrated that privacy policies and other published terms detailing how data is used are often inaccessible to children.[16][17]

While it is an important and welcome principle that information should be given to data subjects about significant decisions taken through solely ADM (AI explainability), it is essential that this is meaningful and personalised so that a child or their parent can exercise their right to contest those decisions, and the right to seek human intervention at the request of the data subject. The current drafting of the Bill leaves this vague.

In a recent judgement of the Court of Justice of the European Union (CJEU) on the GDPR,[18] which UK GDPR derives, the court ruled that data subjects requesting information regarding the use of their data in ADMs should include a description from the data controller about the procedure and principles applied in a system delivered in a way that is "concise, transparent" and "intelligible." It would be appropriate for the Bill to also reflect these requirements.

The code of practice on AI and automated decision-making must be brought forward as soon as possible

[13] Information Commissioner's Office (ND) *What about fairness, bias and discrimination?*

[14] See: IBM (2023) *Shedding light on AI bias with real world examples,* in particular 'Cognitive Bias'

[15] Bogert, E., Schecter, A. & Watson, R.T. (2021) *Humans rely more on algorithms than social influence as a task becomes more difficult*, Scientific Reports, Vol. 11, DOI: https://doi.org/10.1038/s41598-021-87480-9

[16] Revealing Reality (2024) *Children's Data Lives 2024: A report for the ICO*

[17] 5Rights Foundation (2021) *Tick to Agree – Age appropriate presentation of published terms*

[18] European Court of Justice (2025) *C-203/22 Dun & Bradstreet Austria*, Judgement

During Report Stage in the House of Lords, the Government committed to the introduction of a code of practice on AI and sole automated decision-making which will "include guidance about protecting data subjects, including children."[19]

Whilst we disagree with the Government's inclusion of this clause in the Bill, and remain deeply concerned about the implications for children, a code of practice on AI and sole automated decision-making has the potential to clearly set out the expectations and safeguards AI and automated systems making decisions about, or relating to, children.

The Government has said it would table secondary legislation instructing the ICO to produce this code following the Bill's passage.[20] However, owing to the implications for children's privacy, it is crucial that the Government lays secondary legislation as soon as possible.

2. Protecting children's data from commercial use in scientific research

Clause 67 (meaning of research and statistical purposes) **and Clause 68** (consent to processing for the purposes of scientific research) would liberalise the use of personal data for scientific purposes. The new definition includes *"any research that can reasonably be described as scientific, whether publicly or privately funded, and whether carried out as a commercial or non-commercial activity."*

The original definition in Clause 67 was broad and could, without safeguards, be used by tech companies to build commercial products or scrape data for use in AI models to use without consent under the guise of 'scientific research.'

In the House of Lords, peers introduced a new amendment led by Viscount Colville of Culross[21] to state that research can "*only include processing for the purposes of a study* [...] *where the study is conducted in the public interest.*"[22] This clarification narrows the breadth of research covered by this clause and would impose more restrictions on the instances where children's data could be used for commercial activity – including by AI companies seeking to mass-scrape data for their models.

However, in Second Reading of the Bill in the House, the Secretary of State announced that the Government would seek to overturn this change on the basis that "many groundbreaking discoveries come from research with no clear public benefits at the start."[23] This minimises the importance of safeguards for protecting children's data – the Government must ensure that these amendments remain in the Bill to keep the scope of data processing for scientific research watertight and there is no presumption that children are allowed to be used as test subjects.

[19] Lord Vallance of Balham (21 January 2025) *Data (Use and Access) Bill, Report Stage (1st Day)*, col. 1692

[20] Ibid.

[21] Viscount Colville of Culross' amendment, Clause 67, see also: Viscount Colville of Culross (21 January 2025) *Data (Use and Access Bill), Report Stage (1st Day)*, cols. 1632-1634

[22] Clause 67, 3(b), Data (Use and Access) Bill

[23] Peter Kyle (12 February 2025) *Data (Use and Access) Bill, Second Reading*, col. 291

Related to this, **Clause 77** (Information to be provided to data subjects) would allow data controllers to process data for scientific research without providing information to the data subject – meaning tech companies would not have to let subjects know their data has been used for this purpose.

3. Enforcing data protection by design and default for children

Clause 81 (Data protection by design: children's higher protection matters) would amend Article 25 of UK GDPR[24] about data protection by design and by default to strengthen protections explicitly for children's personal data. The clause creates a duty for online services to design their services taking into account specific 'higher protections for children' (in particular regarding to data processing and their rights) and their needs at different ages and developmental stages.

The clause, tabled by the Government alongside Baroness Kidron, gives legal basis to the underlying principles of the UK's Age Appropriate Design Code (AADC),[25] meaning online services that are likely to be accessed by children **should** adhere to its 15 standards. This was also reflected by Lord Vallance of Balham, the Minister for Science, Research and Innovation, who said during Third Reading:

> **"Organisations that are already complying with the [Age Appropriate Design] code should not find it difficult to comply with the new duty, but organisations that have treated compliance with the code as optional will now be under a clear legal duty to design their services with children's rights and interests in mind."**[26]
>
> Lord Vallance of Balham

The AADC has already led to a number of significant design changes in the name of children's privacy and safety.[27] This includes setting children's profiles to private by default, limiting harmful content pushed by recommender systems and prohibiting advertising based on profiling.[28]

However, although the evidence for the AADC's impact is plentiful,[29] so too is evidence of non-compliance. The ICO's *Children's Data Lives* research[30] found tech companies fail to support children to understand how personal data is being used through inaccessible

[24] Information Commissioner's Office (2023) *Data protection by design and default*

[25] Information Commissioner's Office (2021) *UK Age Appropriate Design Code*

[26] Lord Vallance of Balham (5 February 2025) *Data (Use and Access Bill), Third Reading*, cols. 698-699

[27] *Impact of digital regulation on children's digital lives*

[28] See: 5Rights Foundation (2024) *Celebrating 3 years of the Age Appropriate Design Code*

[29] *Impact of digital regulation on children's digital lives*, see also: Children and Screens (2024) *UK Age-Appropriate Design Code: Impact Assessment*

[30] Revealing Reality & Information Commissioner's Office (2024) *Children's Data Lives – Year 1*

privacy policies,[31] disguise the sharing of children's personal data by using design features such as gamification and illustrations,[32] and allow for live location-sharing to be considered the norm among children.[33] Above all, the research highlights that the tech industry continues to absolve itself of any responsibility and place the onus purely on parents to keep their children safe online.

Despite this, the ICO has failed to meaningfully enforce the AADC. Whilst we welcome the announcement of investigations into TikTok, Imgur, and Reddit for potential breaches of the Code,[34] in our response to the ICO's strategy on the AADC[35] we note that the regulator is yet to issue a single fine in relation to breaches of the Code.

In light of Clause 81, we would expect the ICO's enforcement should be steadfast. However, in response to the change, the ICO published a statement[36] indicating that this change will not place children's heightened data protection on a legal footing – in direct contradiction of Parliament and the Minister's remarks that: "organisations that have treated compliance with the code as optional will now be under a clear legal duty to design their services with children's rights and interests in mind."[37]

Urgent clarity must be given from the Government in setting out the expectations of the regulator with regard to this duty and the AADC more broadly. For regulation to work and drive the industry-wide changes needed to protect children online, the ICO must be prepared to enforce more robustly, openly and distinctly to send a message to the public and industry that action is being taken.

4. Protecting children's data in EdTech

We welcome that, alongside an AI and automated decision-making code of practice, the Government will require the ICO to produce an EdTech code of practice.[38] In previous iterations of this Bill, 5Rights, alongside the Digital Futures for Children Centre, have called for the creation of a code of practice to set guardrails in a widely unregulated sector.[39]

[31] *Standard 4 (Transparency), Age Appropriate Design Code* requires services to do provide privacy information, terms of service, policies and community standards in "concise, prominent and clear language suited to the age of the child."

[32] *Standard 13 (Nudge techniques), Age Appropriate Design Code* requires services not use nudge techniques that "exploit unconscious psychological processes (such as associations between certain colours or imagery)" to "encourage children to provide unnecessary personal data or turn off privacy protections."

[33] *Standard 10 (Geolocation), Age Appropriate Design Code*, requires geolocation to be 'off' by default, providing obvious signs for tracking when it is on, defaulted to 'off' at the end of each session.

[34] 5Rights Foundation (2025) *TikTok, Reddit and Imgur investigated for UK Age Appropriate Design Code breach*

[35] 5Rights Foundation (2024) *ICO's Children's Code Strategy 2024-25: 5Rights response*

[36] Information Commissioner's Office (2025) *Information Commissioner's updated response to the Data (Use and Access) (DUA) Bill – House of Commons*

[37] Lord Vallance of Balham (5 February 2025) *Data (Use and Access Bill), Third Reading*, cols. 698-699

[38] Lord Vallance of Balham (28 January 2025) *Data (Use and Access) Bill, Report Stage (2nd Day)*, cols. 148-150

[39] See: Livingstone, S., Hooper, L. & Atabey, A. (2024) *In support of a Code of Practice for Education Technology: Briefing by the Digital Futures for Children centre for Amendment 146 to the Data Protection and Digital Information Bill*

EdTech is becoming a permanent fixture in children's schooling and education. The proliferation of new products was boosted during the lockdowns of the COVID-19 pandemic which contributed to a huge expansion of the market.[40] However, it is largely untested, unregulated, and unaccountable, and exempt from key legislation, including the Online Safety Act, and its inclusion in the scope of the Age Appropriate Design Code is not definitive in every case.[41]

The risks posed to children's data from unaccountable EdTech have real-life consequences. In September 2023, there were calls to shut down the Think Family Education (TFE) app used in Bristol schools[42] which were able to "monitor and profile" pupils based on their family's socioeconomic background or ethnicity, creating a higher risk of discrimination against children and families from these specified groups. In February 2024, an alleged data breach on the EdTech app Class Charts[43] allowed parents and staff to view children's data not related to them – compromising children's privacy and safety.

Research conducted by 5Rights and the Digital Futures Commission[44] identified the risks EdTech presents to children and their data, using Google Classroom and ClassDojo as case studies. It found:

1. **It is impossible to know or discover what data is collected by EdTech providers**: Legal documents governing Google Classroom and ClassDojo's data processing make it difficult to grasp the types of data are collected and the purposes for doing so.
2. **EdTech profits from children's data**: EdTech blurs the boundaries between privacy-preserving and commercial parts of services – e.g. Google Classroom and YouTube or Google Maps – encouraging children to into more commercial environments without highlighting the consequences to their privacy and safety.
3. **EdTech policies do not comply with data protection**: Complicated and multi-layered legal documents make it difficult to decipher privacy policies and/or legal terms, and there is insufficient transparency about data processing.
4. **Regulation gives schools the responsibility but not the power to control data processing**: In several cases, contracts with schools from EdTech providers describe schools as data controllers, despite lacking the power and technical knowledge to determine or direct data processing. The report found that ClassDojo was able to use this loophole.

[40] See: West, M. (2023) *An ed-tech tragedy? Educational technologies and school closures in the time of COVID-19*, UNESCO, DOI: https://doi.org/10.54675/LYGF2153, pp. 28-31

[41] ICO (2023) *The Children's code and education technologies (EdTech)*

[42] The Guardian (2023) *Call to shut down Bristol schools' use of app to 'monitor' pupils and families*

[43] BBC News (2024) *Explicit comments on school app after apparent hack*, see also: SchoolsWeek (2024) *Reports of data breach on Class Charts platform*

[44] Hooper, L., Livingstone, S., and Pothong, K. (2022) *Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo*, Digital Futures Commission, 5Rights Foundation

Despite the risks presented by children's data, it is difficult to prove the unfounded claims made by EdTech providers that their products actually lead to observable improvements in children's learning, attainment or development.

Research conducted by the Digital Futures Commission[45] found there was general uncertainty about the benefits among teachers, and that there was no consensus on the kind of education they wanted from EdTech. Experts are concerned that use of data processing in EdTech is 'too often beneficial to neither children and their teachers,'[46] and that it is difficult to pinpoint what interventions by EdTech may improve the educational outcomes of individual children.

Owing to the known data risks associated with current EdTech practices, it is pivotal that the Government brings forward secondary legislation for the EdTech code of practice **as soon as possible**, setting clear timescales for its delivery. This is necessary for guaranteeing the protection of children from the commercialisation of their data by EdTech, offering clarity for the millions of children, families and teachers impacted by these services in their day-to-day lives.

5. Protecting children's intellectual property from an AI 'free for all'

In December 2024, the UK Government launched a consultation[47] proposing to change existing laws around copyright and intellectual property (IP). The proposed new approach would allow AI companies to use intellectual property and copyrighted works where users have not expressly given their permission to do so, including children.

As early digital pioneers, children are already using AI technologies in all aspects of their lives – from socialising with friends[48] and playing at home to learning at school.[49] This early uptake, their natural curiosity and their still developing cognitive function means that they are much more vulnerable to risks of harm we know these technologies can pose.[50][51] Despite this, children are nowhere in the conversations that the Government, industry or society is having about AI, or the Government's plans to see these systems adopted wholesale into the economy and public services.[52]

We are concerned that the Government's proposed approach will not offer children robust protection from companies seeking to use their work for commercial purposes.

[45] Digital Futures Commission (2021) *Addressing the problems and realising the benefits of processing children's education data: Report on an expert* roundtable, pp. 7-8

[46] Ibid.

[47] Department for Science, Innovation and Technology (2024) *Copyright and AI: Consultation*

[48] Ofcom (2024) *Online Nation: 2024 Report*, pp. 32-38

[49] National Literacy Trust (2024) *Children, young people and teachers' use of generative AI to support literacy in 2024*

[50] Kurian, N. (2023) *'No, Alexa, no!': designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models.* Learning, Media and Technology, 1-14. DOI: https://doi.org/10.1080/17439884.2024.2367052

[51] NSPCC (2025) *Viewing Generative AI and children's safety in the round*

[52] 5Rights Foundation (2025) *UK's AI Opportunities Action Plan overlooks risks and potential for children*

This runs contrary to children's right to be protected from economic exploitation as called for in the UN Convention on the Rights of the Child,[53] which the UK ratified in 1991. It also infringes on children's right to privacy[54] and their freedom of expression.[55]

This is particularly important in the context of the increasing use of AI in schools. At present, the Government plans to create a 'content store' for AI and education technology (EdTech) developers trained on children's assessments[56][57] do not address how these proposals interact and meet children's rights and needs. Given what we know about the existing practices of the EdTech industry to over-collect, overuse and profit from the misuse of children's data,[58] the Government must not allow for a 'free for all' of children's IP without any intervention for children, their parents or their teachers.

Further, the Government's approach contradicts the views of parents and children identified in its own research,[59] which reveals that parents and children have little trust in tech companies for them to be granted control over AI for the use of their children's work and data.[60] Participants assumed that tech companies, without adequate oversight, would sell on their data with little concern for children's privacy and wellbeing.[61] The Government's data mining exception does little to alleviate these concerns.

As part of the research, children themselves shared that they were uncomfortable with their IP being used in schools. In particular, one student noted it was:

> **"Not okay to share [homework] – because your schoolwork is your intellectual property, it's you and you did that. If the AI takes that then you can't copyright it."[62]**
>
> Post-GCSE pupil, Birmingham

The Government must rethink its proposals to ensure that children's IP is robustly safeguarded, particularly in schools where there is an expectation they will be safe from harm and commercial exploitation. In our increasingly digitised world, this is now the only period and place in a child's life where they have a reasonable expectation to not be exploited in this way.

[53] United Nations (1989) Convention on the Rights of the Child, Article 32

[54] Ibid, Article 16

[55] Ibid, Article 13

[56] Department for Education (2024) *Teachers to get more trustworthy AI tech, helping them mark homework and save time*

[57] Department for Education (2025) *AI teacher tools set to break down barriers to opportunity*

[58] West, M. (2023) *An Ed-Tech Tragedy? Educational technologies and school closures in the time of COVID-19*, UNESCO

[59] Responsible Technology Adoption Unit & Department for Education (2024) *Research on public attitudes towards the use of AI n education*

[60] Ibid, p. 32

[61] Ibid

[62] Ibid, p. 25

For more information, please contact:

Reece Parslow
UK Public Affairs Officer
reece@5rightsfoundation.com | www.5rightsfoundation.com

About 5Rights Foundation

5Rights develops new policy, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives and ensures that children's rights and needs are recognised and prioritised in the digital world. While 5Rights works exclusively on behalf of and with children and young people under 18, our solutions and strategies are relevant to many other communities.

Our focus is on implementable change and our work is cited and used widely around the world. We work with governments, inter-governmental institutions, professional associations, academics, businesses, and children, so that digital products and services can impact positively on the lived experiences of young people.

5Rights is a registered charity. Charity number: 1178581.