Consultation response

5Rights consultation response to the UK National Data Strategy (NDS)

We are grateful for the opportunity to provide views and evidence in response to this consultation.

5Rights Foundation speaks specifically on behalf of and is informed by the views of young people. Therefore, our comments reflect, and are restricted to, the ways in which the National Data Strategy will affect young people under the age of 18. However, we recognise that many of our views and recommendations are relevant to other user groups and we welcome any efforts on the part of the government to make the digital world more equitable for all user groups, particularly the vulnerable.

About 5Rights Foundation

5Rights Foundation develops new policy, creates innovative projects and challenges received narratives to ensure governments, the tech sector and society understand, recognise and prioritise children's needs and rights in the digital world. In all of our work, a child is anyone under the age of 18, in line with the UN Convention on the Rights of the Child.

Our work is pragmatic and implementable, allowing us to work with governments, intergovernmental institutions, professional associations, academics, and young people across the globe to build the digital world that young people deserve.

Responses to Consultation Questions

1. **To what extent do you agree with the following statement: *Taken as a whole, the missions and pillars of the National Data Strategy focus on the right priorities.***

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

Strongly disagree.

The National Data Strategy sets forth an agenda that prioritises data availability and sharing over data ethics, user protections and trust.

The idea that greater data availability is an unmitigated societal good is a dangerous one. While recognising the benefits data processing can bring, they must be balanced with individual and societal needs. The strategy's framing of data as an untapped resource to be harvested for maximum economic benefit shows a worrying disregard for the potential harms to individuals or communities of people caused by greater data availability and fails to offer specific protections that are necessary for universal trust in a wider cultural shift towards a data-driven society. Children, that is anyone under the age of 18, have specific rights United Nations Convention on the Child (UNCRC),[1] and specific Data Protections Rights under the ICO's Children's Code.[2] The National Data Strategy must consider children's needs, embody their existing rights, and make an explicit commitment to protect their rights to safety, privacy, and wellbeing.

While encouraged by the inclusion of 'responsibility' as one of the pillars of effective data use, the strategy's overwhelming emphasis on greater data accessibility reduces privacy matters to a minimum and characterises existing protections as 'barriers' to the better use of data. Although Mission 2 looks at public confidence in how data is used, the issue of trust is considered primarily in relation to the pursuit of a pro-growth regime, not as an issue in its own right. Similarly, Mission 4 addresses issues of security and resilience only in the context of data infrastructure, not as issues in their own right that cut across the digital ecosystem. The strategy's primary focus must be on protecting and benefiting the individuals and communities whose data is being gathered and shared, rather than protecting the data itself. As Professor Mary Aiken rightly points out, "your data does not suffer from low self-esteem, self-harm or suicidal ideation."[3]

[1] https://www.unicef.org.uk/wp-content/uploads/2016/08/unicef-convention-rights-child-uncrc.pdf
[2] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/executive-summary
[3] https://thepsychologist.bps.org.uk/volume-33/november-2020/social-diatribe

The strategy should give greater consideration to the potential trade-offs of data availability and explore in more detail the impact of these trade-offs, as well as offering a vision of how we will mitigate the risks associated with increased data sharing and processing. Such risks include the unlawful sharing of personal data, discriminatory or biased outcomes from automated decision-making, the asymmetry of power between data processors and individual users or communities and government uses of public data. Failure to do so will damage public confidence in how data is used and have a significant and specific impact on UK children.

It is vital this strategy does not use the coronavirus pandemic or Britain's departure from the European Union to bring in a new data regime that undermines existing protection to data privacy afforded by the Data Protection Act 2018. Nor should the strategy use the potential benefits of greater data availability as a justification to relax existing regulation protecting the data privacy of children as set out in the ICO's Children's Code.

5Rights recommends the National Data Strategy add a further mission dedicated to upholding data privacy, security and protection that puts citizen trust at the heart of the strategy. Included in this mission should be a commitment to upholding the data protections afforded by the Data Protection Act 2018, including the Children's Code.

2. We're interested in examples of how data was or should have been used to deliver public benefits during the coronavirus (COVID-19) pandemic, beyond its use directly in health and social care. Please give any examples that you can, including what, if anything, central government could do to build or develop them further.

The Education Sector

The use of automated decision-making in grading GCSE and A-level results in the summer of 2020 introduced algorithmic bias into the examination process with catastrophic consequences for the government, education sector and, most significantly, children. The algorithm determined results using data from schools' past performances and ranked children of a similar ability differently, which had a disproportionately negative effect on state schools that had a greater number of pupils of similar ability. Failure to take advice from the exam regulator and hasty implementation resulted in widespread 'downgrading', particularly of those who were at the margin of grades. The government's policy focus on grade inflation made it blind to the needs of students looking for a true reflection of their individual attainment. Crucially, presenting such uses of data as policy 'neutral' resulted in outcry, with policies being reversed as the impact of processing priorities become evident. If society is to benefit from government use of data-driven technology, greater transparency is needed on how and to what purpose data is used and algorithms are built, as well as careful implementation, clear accountability and robust governance processes.

Also in education, a more robust data strategy could have helped the Department for Education to facilitate remote learning during the coronavirus pandemic. Many disadvantaged children were left behind in the shift to remote learning, with insufficient access to devices, connectivity (broadband or data) and to online learning resources. Swifter action to ensure all children had access to resources would have saved anxiety for many families, teachers and students and avoided regressions in learning. At the same time as those on the frontline struggled with access, it emerged that there were insufficient protections in place to eliminate risks and harms to young people learning remotely.

While the government introduced emergency legislation under the Coronavirus Act 2020 to mandate remote learning, it failed to introduce emergency protections, leaving children and teachers exposed to risk. A significant number of remote learning platforms offered no explicit protections for children's data and their right to privacy, and shared data with third-parties for commercial purposes.[4] Poor security settings also left teachers struggling with inappropriate, and sometimes illegal material entering the remote classroom. Remote and online learning is likely to be a growth area for the foreseeable future. It provides a clear example of why an additional, balancing mission on security and privacy is a prerequisite for a successful and equitable data strategy.

Digital and data literacy are an important part of supporting children to understand the consequences of data sharing, but the responsibility for mitigating harm must not be placed on those most likely to experience it. It is inappropriate to educate young people to use a world which systematically asks them to act beyond their maturity and puts them at risk, and it is unreasonable to transfer responsibility for staying safe to children who are forced to deal with a complex system where risks are created by design, not only by user behaviour.

There are clear benefits to be realised from better use of data in the delivery of public services, particularly in education settings, but the government must be transparent about how its policies are being delivered through automated processes. It must consult and test with experts before employing automated decision-making processes, and invite public scrutiny through the publication of the advice they have received, alongside the source code or statistical models they propose to use.

5Rights recommends the creation of a sector-wide code for use of data, devices and digital services in the education sector. Additionally, guidance for automated assessment should be created and tested in multiple education settings.

3. If applicable, please provide any comments about the potential impact of the proposals outlined in this consultation may have on individuals with a protected characteristic under the Equality Act 2010?

[4] https://digitalwatchdog.org/wp-content/uploads/2020/09/IDAC-Ed-Tech-Report-912020.pdf

Children are vulnerable by virtue of their age and developmental capacity, which affect their ability to understand the complexity of data processing. Children must therefore be considered as a vulnerable group for the purposes of the National Data Strategy.

Children's rights are routinely violated online. Manipulative data collection, storage, and usage practices, data-driven design features and automated decision-making processes, including nudge techniques, profiling, and recommendation loops, can infringe on a child's privacy. Moreover, features that recommend adults befriend unknown children, or prioritise children's profiles and content in recommendation feeds to users who have shown a previous interest in young people,[5] or to users who had watched sexually themed videos in the past, present serious threats to a child's right to protection from harm.

The National Data Strategy is focussed on making personal and whole community data available, to what will inevitably be a mix of government, civic and commercial organisations. It is imperative that in doing so it does not add to the 'digital footprint' of an individual child, or further enable the violations set out above. A National Data Strategy that puts children at further risk will be a failure of government's first duty to keep its citizens safe. Of note is that vulnerable children and children from lower socio-economic backgrounds are more likely to experience harms associated with data processing. For example, students from disadvantaged areas were disproportionately affected by the algorithm that generated A-level results, and looked after children are seven times more likely than other children to have their personal details hacked or stolen.[6]

These children need the government to ensure that the National Data Strategy takes specific and robust steps to ensure that their rights are not violated, including but not limited to, their rights to privacy and protection from violence and harm.

5Rights recommends that the National Data Strategy makes a formal commitment to uphold the UN Convention on the Rights of the Child, and specifically cites the Convention's upcoming General Comment on the Digital World.

4. We welcome any comments about the potential impact of the proposals outlined in this consultation on the UK across all areas, and any steps the government should take to ensure that they take account of regional inequalities and support the whole of the UK.

It is estimated that 22% of the UK population lack the necessary digital skills to navigate an increasingly digitalised world.[7] For children, lack of access and support in the digital environment may undermine their enjoyment of school, their academic outcomes, their right to health and wellbeing and their future employment prospects.[8]

[5] https://www.nytimes.com/2019/06/03/world/americas/youtube-pedophiles.html
[6] https://www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Report-Vulnerable-Children-in-a-Digital-World.pdf
[7] https://www.cam.ac.uk/stories/digitaldivide
[8] https://fdslive.oup.com/www.oup.com/oxed/wordgap/Bridging_the_Word_Gap_at_Transition_2020.pdf?region=uk

These inequalities have geographic as well as socioeconomic patterns, particularly but not exclusively in remote areas where access to fast broadband is limited.

The coronavirus pandemic has exacerbated the UK's digital divide. As many as 1.78 million children in the UK had no access to a laptop, desktop or tablet at home to use for remote learning.[9] In disadvantaged areas, the number of children without exclusive access to their own device can be as high as 47%.[10] When a child uses another person's device or a parent or guardian's account, the device or service-level protections afforded to children can be compromised, presenting risks to their personal and data privacy. The government should build on DfE's laptops for disadvantaged children programme and create meaningful and ample provisions to ensure no child is left behind or exposed to risk.

Children should not have to make the choice between their rights to education and participation and their rights to privacy and protection. The National Data Strategy must address access issues - to devices and broadband/connectivity, in tandem with online protections - if data is to drive better outcomes for all across the UK.

5Rights notes that the role out of laptops and the new rules for remote learning during the pandemic were not accompanied by sufficient additional safeguarding. In particular, the government failed to set minimum standards for the design of services and platforms used for remote learning, or social media companies that were recommending harmful content to children too young to be on their service.

5. Which sectors have the most to gain from better data availability? Please select all relevant options drawn from the Standardised Industry Classification (SIC) codes.

Information and Communication

The information and communication sector has much to gain from better data availability, but realising these benefits should not be at the expense of a child's right to data privacy and protections.

The majority of the tech sector is in the business of using data for the purposes of prediction and persuasion, seen most visibly through the use of profiling, targeting advertising and recommendation features. These features use personal data points and aggregated data sets to predict user behaviour and guide users to choose a certain course of action. What is euphemistically termed "better use of data" in this strategy could be interpreted by companies whose business models rely on the aggressive mining and selling of data, as carte blanche to continue unscrupulous data processing activities.

[9] Estimated statistic provided by One Laptop report, October 2020.
[10] Tackling Digital Disadvantage, OneLaptop.org, October 2020

Many aspects of human behaviour have now been commodified, with data as the currency. From monitoring sleep patterns to tracking mood, data processing has encroached on many intimate aspects of our lives, often with damaging consequences. The negative impact of these data practices is felt across society, but most acutely by children and young people. Exposure to harmful content, excessive engagement, unintended or uncontrolled spending through in-service purchases and the exponential rise in online hate and misinformation are just a few examples of the harmful effects these data practices have on children and young people.

The National Data Strategy must ensure it does not further embed these practices and acknowledge the important principle of data minimisation in relation to children's data, as set in in the Children's Code.

Education

EdTech is a fast-growing market, with the demand for online learning platforms growing exponentially in the wake of the coronavirus pandemic.[11] Data-driven features of EdTech services have led to a number of unacceptable data processing practices, including the activity tracking of children both in the classroom and at home, discrimination against marginalised students and the sale of data to third parties.[12] 58% of EdTech services used globally pose a high risk to children's data, with 75% containing in-service ad tracking, 79% containing open-ended or undisclosed data retention time limits, and 58% of services storing location information.[13] We have allowed these harms to come to children in a space that is designed for safe learning. It is vital that in a sector that has much to gain from greater availability of data, children do not stand to lose their rights to safety and privacy.

Justice

The use of data for automated decision-making is becoming more prevalent in the criminal justice system, from identifying likely criminals to guiding court sentencing. The use of big data and algorithms have the potential to increase efficiency and consistency across the justice sector, but they also present an equal and opposite risk to entrench poor practice and embed poor data. This is seen in the Metropolitan Police Service's gang-mapping database, known as the Gangs Matrix, which used algorithmic profiling to identify individuals likely to be involved in criminal activity. The monitoring of young people's behaviour online to determine gang affiliation resulted in teenagers being profiled and tracked by police based on the content they consumed and the people with whom they associated online. Amnesty International described the Gangs Matrix as "a racially biased database criminalising a generation of young black men."[14]

[11] https://en.unesco.org/covid19/educationresponse
[12] https://theconversation.com/childrens-privacy-is-at-risk-with-rapid-shifts-to-online-schooling-under-coronavirus-135787
[13] https://www.top10vpn.com/research/investigations/remote-learning-privacy/
[14] https://www.amnesty.org.uk/press-releases/met-police-using-racially-discriminatory-gangs-matrix-database

For justice to be served and to be seen to be served, a robust system of transparency, oversight and careful auditing is critical. Importantly, automated systems cannot be used primarily for cost cutting purposes, but rather be built with significant safeguards from the start to provide a better and more efficient system. Only this will give long-term public confidence in the justice system. We are encouraged by the draft strategy's commitment to ensuring that data's potential is harnessed to drive a better, more inclusive and less biased society rather than entrenching existing problems, and hope to see this reflected in the government's approach to the implementation of data-driven technologies.

In all the above sectors, and more, intelligent uses of data have the potential to support the provision of services, drive resources to where there is need, and allow new connections between different sources of information to benefit the UK. However, citizens are ruled by consent, and a data strategy that is solely focused on creating efficiencies or commercial benefits that fails to create systems of trust, transparency and accountability are likely to be rejected and will take longer or fail entirely to provide the ultimate benefits of a connected society.

6. What role do you think central government should have in enabling better availability of data across the wider economy?

With greater availability of data must come better safeguards and protections of personal data. Central government has a critical role to play in mitigating the effects of greater data availability on the security, privacy and wellbeing of data subjects. In particular, it has a duty to uphold and enforce the protections afforded to children and other vulnerable user groups in the Data Protection Act 2018 and under the UN Convention on the Rights of the Child.

Manipulative data collection practices are an industry norm. All too often services have low default privacy settings and incomprehensible terms of use that are rarely read and poorly upheld,[15] making it difficult for users to exercise any real control over their data. For example, it takes a user 17 clicks to opt out of Google's data collection in the United Kingdom, while it only takes one click to consent to all data being collected. The government has a role to play in setting minimum standards for data collection and processing that are systemic in nature and have the flexibility to take account of new and emerging risks. These standards should include:

- Privacy and safety settings that are high by default
- Prohibited use of bundled consents, or nudges that encourage lower privacy settings
- Data minimisation principles that allow sharing of beneficial and specific data but does not lead to additional or unnecessary 'harvesting' of a user's personal data or user group data.

[15] https://www.vice.com/en/article/xwbg7j/online-contract-terms-of-service-are-incomprehensible-to-adults-study-finds

- Published terms that are presented in ways that are truthful, easily understood and accessible to young people, and at times when they are most likely to engage
- Accountability for services to uphold community guidelines, terms and conditions, and privacy notices
- Adequate and child-appropriate means of redress for victims of unlawful data processing.
- Limitations around third party data sharing (a data sharing regime that ensures citizens are not scared or reluctant to share data with government for a specific purpose for fear it will then be shared with commercial companies or organisations.)

As well as introducing minimum standards, the government should ensure independent regulators have algorithmic oversight of data-driven technologies and services, particularly those that impact on children and other vulnerable data subjects. Automated decision-making systems are embedded in many digital services. These systems collect and analyse data to predict user behaviour and persuade users to follow a certain course of action, or they may impact on them indirectly, such as facial recognition in public settings. The government has a duty to ensure oversight of these systems, to ascertain their purpose and the nature and presence of harms they cause, to identify and assess the data used to train algorithms (and how it is collected), to analyse the source code and/or statistical model in use and to conduct its own tests to assess how an algorithm operates in practice and over time. This oversight must be transparent, consistent and enforced.

Data sharing *and* the oversight regime needs to have the trust of the population to be successful. The government must require service providers to be transparent about the purpose of data gathering, processing and sharing activities, to ensure this information is communicated in a way that is understandable to non-experts, and to provide users with an easy way to 'opt-out' of a service's data collection.

Whilst we welcome the long awaiting Online Harms Bill, government could and should act faster, using existing regulatory mechanisms to introduce guidance/regulation on minimum standards, including design principles, fairness and presentation of published terms (including age restrictions and community rules), child-appropriate moderation and redress, age assurance, child impact assessments and effective governance and accountability. It must adopt a 'child first' approach when developing tech policy and use its powers to enforce requirements on companies, and to investigate services that fail to meet these standards.

Public trust in government use of data, whether real or perceived, will determine the success of any new data regime. It is imperative that the government considers public trust – and the safeguards, assurances and protections to secure that trust – not only as a pillar to effective implementation but as the very foundation on which to build its data regime. Unless and until government acts to protect children, their data and their online experience more broadly, there will be a natural resistance to the further sharing of their data. Children are one fifth of all online users in the UK and spend a greater

amount of time online than other demographics. To create "the optimal environment for data to drive growth and productivity in the UK", the government needs to give primary consideration to the needs of those upon who's trust this strategy relies.

5Rights recommends the government invest in the enforcement of current legislation applying to digital services and uses existing regulatory mechanisms to introduce a set of minimum standards to which service providers must adhere, and to grant independent regulators algorithmic oversight of services that use automated decision-making systems.

6a. How should this role vary across sectors and applications?

The online experiences of children take place across the digital world and are not limited to child-directed services. Any and all online services that create risks or facilitate or cause harms to children must be subject to regulatory standards, regardless of the intended audience or the nature of the organisation that owns that service. This includes search engines, online gaming sites, business-to-business services, online shops, pornography websites and private messaging services, as well as privately and publicly held data sets.

Regulatory standards should apply to all organisations that process data or design services based on the collection and processing of data. Additional regulatory oversight must also be applied to automated systems that have an impact on the outcomes of data subjects but may not be transparent to the end user, such as local authority services, educational assessments or financial services.

Additionally, government should take specific action to protect vulnerable users, noting that in different digital environments and services, different groups may be vulnerable. Those groups may include, women, older people, users from low socio-economic backgrounds, those without access or digital skills, those who can be identified by their ethnicity or religious background, users with accessibility needs – and children.

Where data subjects are more likely to be children, such as in education technology services or social networks popular among young people, the government should pay particular attention to the design of services and the potential risks posed by their data processing practices. Enforcement mechanisms should be proportionate to the risks that services pose to young people and reasonable efforts taken to avoid and mitigate risks should be recognised.

5Rights, as part its work on the Digital Futures Commission, is developing recommendations for child-rights-respecting data governance mechanisms that can unlock the potential of education data. We invite policymakers from Department for Education and across government to join this research collaboration to support innovative uses of education data that serve the interests of children and young people.

7. To what extent do you agree with the following statement: *The government has a role in supporting data foundations in the wider economy.*

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

Somewhat agree

The government should have clear regulatory oversight over data foundations, particularly those that intersect or are in some way sponsored or enabled by big tech or commercial companies that carry out or benefit from data processing. If data is held by mutual cooperatives among communities and individuals, then the government has a role to play in supporting the governance and fair terms of such organisations. It should also ensure that UK regulators have information gathering powers and oversight in a manner set out in 5Rights' Priorities for the Online Harms Bill.[16]

Building on ADR-UK's work to transform researcher access to public sector data, the government should develop open systems through which academics and civil society can access privately held data. Improving appropriate access to privately held data foundations will facilitate and promote research and innovation, unlocking significant economic and social benefits for the UK.

If supporting data foundations in the wider economy is synonymous with commercial enterprises realising value from nationally held data, then the government has a role to protect that data and enforce robust regulation to manage its use. The government must uphold the highest bar of ethics, in line with children's rights, when managing and sharing this data, with explicit consent from the public and appropriate transparency to allow for public scrutiny. If citizens withhold information from government for fear of it being sold, share or spread in a way that disadvantages them or violates their privacy, then the strategy will have failed in its ambition to create a trusted data regime.

5Rights recommends that government data foundations are managed with a clear set of protections, and a system of governance that is (structurally and visibly) independent of government, but to which all data foundations, commercial, community and government organisations are subject.

8. What could central government do beyond existing schemes to tackle the particular barriers that small and medium-sized enterprises (SMEs) face in using data effectively?

While greater coordination between services is welcomed, there are obvious risks involved when providers share information about their users with third parties, particularly when those users are children. Data collection and sharing by organisations

[16] https://5rightsfoundation.com/uploads/5rights-priorities---online-harms-bill.pdf

of any size (SME or otherwise) must be carried out with transparency and accountability and underwritten by robust data and consumer protections. As we have indicated throughout this response, greater data sharing would be expedited and better received by the public if there was a stronger commitment to, and understanding of, protecting and promoting the interests of users. In particular, all services that process children's data, including government, must be subject to regulation and oversight.

The positioning of regulation as a barrier to a business' ability to scale is at best unhelpful and at worst, dangerous. In its Online Harms White Paper, the government suggested SME's and start-ups may be exempt from certain regulations designed to prevent the excessive sharing of personal data. This could lead to start-ups such as OnlyFans, that provide a service where young people can sell self-generated sexual content to subscribers, not being subject to regulation, despite now having millions of users accessing and selling sexual content. It is crucial that innovation and regulation are not framed in the strategy as two mutually exclusive concepts. Regulation that drives compliance rather than deals out punishment should be applied to all companies, regardless of size. It is important to note that companies who use data in fair, equitable and safe ways will have little or nothing to do to meet regulatory standards. Making the data ecosystem, fair, trusted and accountable will allow users to share their data more freely and equitably, while supporting the growth of start-ups and SMEs.

While we welcome the development of sector-specific guidance to support industry compliance, the proposed use of "co-regulatory tools" in the draft strategy is cause for concern. In practice, co-regulation often amounts to self-regulation, and as is widely acknowledged, self-regulation across the tech sector has failed to protect users, their security and privacy. Good regulation is enabling, not limiting, so it follows that all commercial enterprises should be subject to data privacy regulation that provides clarity and certainty for companies when handling data.

5Rights recommends SMEs and start-ups are subject to regulatory requirements that are proportionate and risk-based, and supported to grow through the availability of sandboxes, minimum standards, codes of practice and guidance around issues such as harmful outcomes for children.

9. Beyond existing Smart Data plans, what, if any, further work do you think should be done to ensure that consumer's data is put to work for them?

The purported benefits of AI and data-driven technologies to consumers should be considered in relation to the risks of privacy and safety violations that these benefits are accompanied by. In the CDEI's own review into attitudes to online targeting, it was shown that only 28% of people trust platforms to target them in a responsible way, and when they try to change settings, only a third of people trust companies to do what they ask.[17] Algorithms are integral to the experience of the user, but the basis on which they

[17] https://www.gov.uk/government/news/cdei-calls-for-overhaul-of-social-media-regulation

'optimise' the user experience is opaque to anyone outside the company providing the service. In fact, algorithms are widely considered to be optimised for the benefit of the commercial interest of the company, not the security or rights of the user. Without algorithmic oversight, it is impossible to ascertain the nature, presence or responsibility for harms experienced by young people.

Commercially driven design features have a disproportionate impact on children who are less able to make informed and conscious decisions due to their age and developmental capacity. The use of algorithms to power aggressive marketing techniques, such as behavioural advertising, profiling, and recommendation loops, present a number of threats to children's rights. For example, there have been countless cases of children's personal data being shared with third parties against the best interests of the child.[18] The use of these automated decision-making systems can lead to unsolicited or inaccurate profiling, inappropriate contact or stalking, exposure to age-inappropriate or harmful content and financial harm. The government must ensure that these harms are identified and mitigated in the use of data for commercial purposes.

5Rights recommends a reframing of this question to focus on the protections that users –particularly children – need to have in place before any sharing can proceed. This should be accompanied by a set of minimum standards for security and informed consent.

10. How can the UK's data protection framework remain fit for purpose in an increasingly digital and data driven age?

In an increasingly digital and data driven age, the UK's data protection framework must consider the 'best interest of the child'[19] as primary to the design and development of digital services. The Data Protection Act 2018 (DPA) overlaps with many of the matters raised in the draft National Data Strategy. The DPA implemented GDPR in the UK, introducing principles and definitions that are fundamental to good data governance, such as purpose limitation, transparency and data minimisation, and introduced ground-breaking (and world leading) data protection for children through the ICO's Children's Code, which created practical and implementable standards built on the principles contained in GDPR. The National Data Strategy should not seek to undermine or row back on these standards and the hard-won protections they support, but rather build on them and allow for flexibility to adapt to a changing data environment.

The UK's data protection framework should include minimum standards for data processing and require organisations to give prior consideration to the impact their services might have on the rights of children, as per the UN Convention on the Rights of the Child. Even in a pro-growth data regime, the principle of data minimisation (set out

[18] https://www.thetimes.co.uk/article/smart-toys-spying-on-children-nc03d8xbm
[19] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/

in Standard 8 of the Children's Code) should be fundamental, where companies collect and retain only the minimum amount of personal data needed to provide the elements of a service in which a child is actively and knowingly engaged. To support organisations to identify the risks that their data processing activities pose to children, the government should introduce mandatory child impact assessments and require services to demonstrate the measures they have taken to minimise or eradicate identified risks.

The government should remain responsive to the development of new technologies but stay service/product neutral when issuing guidance or introducing regulation. It must also take an iterative approach to its data protection framework and take measures to routinely identify and address where the framework is falling short of its stated aim to protect users and their data.

Moreover, the government must have the necessary resources and enforcement powers to ensure organisations, particularly big tech companies, are held to account and face appropriate sanctions when data protection regulations are breached. **The provision of specific data protection for children's data must be accompanied by enforcement of the regulation in which those protections are enshrined.**

5Rights recommends that the government renews its commitment to GDPR, the Data Protection Act 2018, and does not become the "Singapore of data protection" by creating an environment in which only the lowest levels of data protection are given.

11. To what extent do you agree with the functions set out for the Centre for Data Ethics and Innovation (CDEI) – AI monitoring, partnership working and piloting and testing potential interventions in the tech landscape?

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

Somewhat agree

We agree that the CDEI should function as a research base, partnering with organisations to test technologies in a sandbox environment for the purpose of identifying and mitigating risks presented by AI and data-driven technologies. The remit of the CDEI should also include active investigation and mitigation of the risks presented by such technologies, and not be limited to a 'monitoring' function that reacts only after harm has been caused. It should also have information gathering powers that are interconnected and streamlined to support those of Ofcom.

That said, companies and data subjects must not be required to understand the specific remits of the various government actors responsible for setting out and

enforcing data standards to navigate the data regime. We are concerned that the plethora of actors - CDEI, Ofcom, ICO, CMA, Data Advisory Board, Data Standards Office and the new Chief Data Information Officer, as well as specialist sectors including security and health - risk complicating transparency, accountability and governance processes. At a minimum, the strategy must set out clear lines of accountability and enforcement responsibility to ensure regulatory compliance from companies who understand what is required of them, and to secure public trust in the data regime. Consideration should also be given to bringing some of the responsibilities together in a small number of regulators, rather than adding to the government value chain.

11a. How would a change to statutory status support the CDEI to deliver its remit?

Automated systems need regulatory oversight from an independent regulator that has statutory responsibilities, information gathering powers and sufficient resources to provide appropriate levels of oversight and enforcement power. With statutory status, the CDEI could act at arms' length from the executive and Parliament, but have powers to introduce legislation through the laying of statutory instruments, allowing it to respond more quickly and with greater agility to address emerging issues.

If CDEI were given statutory status, it would be bound by the Human Rights Act 1998 and the Equality Act 2010. Section 6 of the Human Rights Act states "it is unlawful for a public authority to act in a way which is incompatible with a Convention right." This would give CDEI a statutory duty to uphold the UN Convention on the Rights of the Child (UNCRC) and consider the best interests of children in all its actions. Under Section 149 of the Equality Act, "a public authority must, in the exercise of its functions, have due regard to the need to eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act." The CDEI would therefore be obliged to act with due regard to the needs of children, who, by virtue of their age and developmental capacity, are vulnerable users of the digital world.

5Rights recommends the CDEI is given a remit and powers that are complementary to those of Ofcom, Information Commissioner's Office and Competition and Markets Authority. Together, they should provide an expert, fully resourced and clearly independent regulatory ecosystem to hold commercial, third sector and government organisations to account.

12. We have identified five broad areas of work as part of our mission for enabling better use of data across government:

- Quality, availability and access
- Standards and assurance
- Capability, leadership and culture
- Accountability and productivity
- Ethics and public trust

We want to hear your views on any actions you think will have the biggest impact for transforming government's use of data.

We are encouraged by the inclusion of standards and assurance as one of the mechanisms for enabling better use of data across government, and would expect these standards to include robust protections of government-held personal data, particularly the data of children and young people. Consideration of ethics and public trust will also be essential for the better use of data in government. Public trust can only be achieved by absolute transparency accountability and redress in the way government collects, stores and processes personal data, and in particular, any data-driven technologies it deploys to make decisions affecting the lives of children.

We note that while government messaging focuses on data itself and the value that might accrue from it, little attention is given to how the government intends to judge the purpose and mechanisms behind data processing, or the view it holds on purpose limitation. It is vital that the strategy aligns value realisation with the interests of data holders and sets out how it intends to measure the benefits of increased data availability and sharing. The strategy as currently set out, does not appear to recognise that it may not always be in the best interests of society to share data, or to process it for a particular purpose, particularly in light of recent issues such as the spread of COVID-19 misinformation, the Facebook-Cambridge Analytica scandal and racial biases in facial recognition. It seems imperative to acknowledge the government's role in ensuring the purpose of data processing, for which it is encouraging data sharing, is in itself, fit for purpose and meets minimum standards.

5Rights recommends the addition of transparency, redress, and a specific mention of government responsibility to vulnerable groups in the strategy, including a commitment to children's rights under the UNCRC, and children's data protection rights under the Children's Code.

13. The Data Standards Authority is working with a range of public sector and external organisations to create a pipeline of data standards and standard practices that should be adopted. We welcome your views on standards that should be prioritised, building on the standards which have already been recommended.

The ICO introduced the Children's Code in September 2020 to explain how the General Data Protection Regulation applies in the context of children using digital services, and to set out standards for data protection in a statutory code of practice. The Children's Code does not currently apply to government-held data processing. This is something the National Data Strategy must address. Not only do many commercial services already use government-held data, but the draft strategy's stated ambition to increase data sharing between government departments and commercial services will make the processing of children's data more widespread. Introducing the Children's Code across all data sets would streamline protections for children and ensure the safeguards implemented by other data processors are not undermined by the government's failure to follow its own standards.

Building on the introduction of the Children's Code, the government should mandate the use of child impact assessments across all digital services, allowing service providers to identify and mitigate risks to children presented by data processing practices. 5Rights is developing a template child impact assessment tool and would welcome the opportunity to work with the Data Standards Authority to introduce child impact assessments as part of the pipeline of data standards and practices to be adopted by service providers.

5Rights recommends that the Children's Code is applied to all government-held data, to streamline data protection for children in the UK.

14. What responsibilities and requirements should be placed on virtual or physical data infrastructure service providers to provide data security, continuity and resilience of service supply?

Data infrastructure service providers should have a legal duty, proportionate to the risk of privacy violations, to ensure the security and resilience of data infrastructures, whether physical or virtual. This is particularly important for service providers that hold the data of children and other vulnerable data subjects. This will require strong central procurement guidance from the Government Digital Service/Cabinet Office and monitoring of compliance from the centre, with strong sanctions both contractually and via the ICO.

We note in question 4 that during the coronavirus pandemic, 1.78 million UK children did not have access to remote learning, either through lack of access to devices or connectivity. The National Data Strategy should seek to bridge this accessibility gap and may wish to work with infrastructure providers as key stakeholders in the value chain.

14a. How do clients assess the robustness of security protocols when choosing data infrastructure services? How do they ensure that providers are keeping up with those protocols during their contract?

Not applicable.

15. Demand for external data storage and processing services is growing. In order to maintain high standards of security and resilience for the infrastructure on which data use relies, what should be the respective roles of government, data service providers, their supply chain and their clients?

In the EU's Network and Information Security Directive, Article 16 states that digital service providers must "take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and

information systems which they use in the context of offering services."[20] The government has a role to play in developing data hosting legislation that recreates the protections UK data subjects currently enjoy under GDPR.

Government must provide strong procurement guidance for companies or public sector organisations wishing to procure data infrastructure services. This guidance must recognise the higher bar of data protection children are given under the Children's Code. For private sector use of data infrastructure, government should establish the requirements for infrastructure security standards and give the ICO adequate enforcement powers to ensure these are followed. Data service providers should also be responsible for demonstrating compliance through monitoring or and auditing.

16. What are the most important risk factors in managing the security and resilience of the infrastructure on which data use relies? For example, the physical security of sites, the geographic location where data is stored, the diversity and actors in the market and supply chains, or other factors.

The concern around the geographical location of data infrastructure sites is that certain countries may attempt to access or interfere with data held in their territory. There is also an increasing understanding that there is a divergence in approach to the protections and oversight of the digital value chain. It is vital that the government retains the right to decide which territories its data can or cannot be held in. This would mitigate the risks presented by lack of regulation and regulatory oversight in other territories.

17. Do you agree that the government should play a greater role in ensuring that data does not negatively contribute to carbon usage?

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

Strongly agree

Today, data centres consume about 2% of electricity worldwide, predicted to rise to 8% of the global total by 2030, and contribute to 0.3% of global carbon emissions.[21] U.S. data centres alone consumed 70 billion kilowatt-hours of electricity in 2014 - the same amount that 6.4 million American homes used that year.[22] The carbon footprint of our gadgets, the internet and the systems supporting them account for roughly 3.7% of

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[21] https://www.nature.com/articles/d41586-018-06610-y

[22] https://fortune.com/2019/09/18/internet-cloud-server-data-center-energy-consumption-renewable-coal/

global greenhouse emissions.[23] This is comparable to the amount produced by the airline industry globally and is predicted to double by 2025.

The impact of climate change will be felt most by children growing up in the world today and by generations to come. Its effects will challenge children's most basic rights and protections: the right to life, survival and development and the right to an adequate standard of living. Article 12 in the UNCRC also states that children have a right to be heard. Children as a demographic feel strongly that climate change is the central issue of their time. Any action taken by the government on this issue will also be fulfilling the rights of children to have their voices heard.

5rights recommends the government play an active role in ensuring that data does not contribute to increased carbon emissions, to safeguard the physical environment in which children live.

18. How can the UK improve on current international transfer mechanisms, while ensuring that the personal data of UK citizens is appropriately safeguarded?

Reaching a data adequacy agreement with the EU is key to ensuring international data flows and to maintaining regulatory standards. There are also considerable concerns that the current data sharing provisions in new trade agreements such as UK/Japan are putting at risk our compliance with the GDPR and therefore the UK's ability to qualify for data adequacy.

In its Free Trade Agreement with the US, the UK must not accept US domestic legislation or standards that offer a lesser standard of data protection and privacy than is currently offered in the UK. The US has introduced a requirement for recipients of US trade deals, including Mexico, Canada and Japan, to accept aspects of a broad *and hugely contested* US domestic law that will unduly benefit the large corporations of Silicon Valley, and prevent them from being held liable for the harm caused by their services. Section 230 of the US Communications Decency Acy is routinely misused by companies to escape their responsibilities to protect users. It is used as a 'get out of jail free card' to continue operating services that present serious risks to children. The influence of Section 230 will threaten to undermine, or at a minimum, put a chill on both existing UK law as well as the much-anticipated Online Harms Bill. We note that the new administration will also be looking at Section 230 and that it would be untimely for the UK to embody a law that is in contention in the US.

The drive to improve international data sharing should not come at the cost of appropriate protections of personal data. The online safety of children and other vulnerable users must not be compromised as a consequence of clauses that appear in Free Trade Agreements, in particular the data protections afforded by GDPR, the

[23] https://www.bbc.com/future/article/20200305-why-your-internet-habits-are-not-as-clean-as-you-think

Children's Code and any additional security offered by the forthcoming Online Harms Bill.

19. What are your views on future UK data adequacy arrangements (e.g. which countries are priorities) and how can the UK work with stakeholders to ensure the best possible outcome for the UK?

The draft strategy sets out the UK's intention to seek EU data adequacy to maintain the free flow of personal data from the EEA and to pursue UK data adequacy with global partners after Britain leaves the EU. Data adequacy agreements are essential to ensure personal data is properly protected, and to continue the UK's participation in European data sharing programmes that protect UK citizens, such as Europol. It is now critical that the government makes a firm commitment to give robust powers to a regulatory body that will meet the European Commission's expectations of an effective supervising authority, in order to achieve a data adequacy agreement with the EU.[24]

As this strategy states, "technical standards are increasingly expressions of ethical and societal values." If the UK is to maintain its reputation in the future as a free, fair and right-respecting society, and achieve its stated aim of being "the safest place in the world to go online", the government must enforce minimum standards of data protection that uphold the rights of children and young people as set out in the Data Protection Act 2018 and Children's Code.

For more information please contact:
Izzy Wick | Policy Lead | izzy@5rightsfoundation.com

Building the digital world that young people deserve

5RIGHTS FOUNDATION

Website: 5rightsfoundation.com
Twitter: @5RightsFound
Email: info@5rightsfoundation.com

[24] https://www.euractiv.com/wp-content/uploads/sites/2/2020/10/Letter-Brexit-Commission-data-ICO-12Oct2020.pdf