Governance of data for children's learning in UK state schools

Digital Futures Commission
June 2021

DIGITAL FUTURES COMMISSION
Innovating in the interests of children and young people

5RIGHTS FOUNDATION

The Digital Futures Commission

The Digital Futures Commission (DFC) is focused on putting the needs and interests of children and young people into the minds and workplans of digital innovators, business, regulators and governments. It calls for a critical examination of how children's lives are being reconfigured by innovation, so as to reimagine the digital world in value-sensitive ways that uphold rights, and to take practical steps to meet children's needs. This document is a snapshot of where the DFC is seeking to make an impact. As the work progresses, and through the process of consultation, we imagine this report will evolve.

The DFC research team is led by Professor Sonia Livingstone OBE.

Commissioners

David Halpern, Chief Executive, The Behavioural Insights Team

Baroness Beeban Kidron OBE, Founder and Chair, 5Rights Foundation

Ansgar Koene, Global AI Ethics and Regulatory Leader, EY

Professor Sonia Livingstone OBE, London School of Economics and Political Science

Professor Helen Margetts OBE, The Alan Turing Institute

Professor Mark Mon-Williams, University of Leeds

Professor Dorothy Monekosso, Leeds Beckett University

Professor Brian O'Neill, Technological University Dublin

Michael Preston, Executive Director, Joan Ganz Cooney Centre, Sesame Workshop

Anna Rafferty, Vice President, Digital Consumer Engagement, The Lego Group

Dee Saigal, Co-Founder and CEO, Erase All Kittens

Farida Shaheed, Shirkat Gah, Women's Resource Centre

Roger Taylor, Chair, Centre for Data Ethics and Innovation

Adrian Woolard, Head of Research & Development, BBC

Full biographies and more details about the Commissioners can be found here.

Suggested citation format: Day, E. (2021). *Governance of data for children's learning in UK state schools.* Digital Futures Commission, 5Rights Foundation.

Funding: The Commission is funded by 5Rights Foundation with funding in kind from LSE. We gratefully acknowledge a contribution from LEGO in 2020/21.

Cover image: 441373651 by wavebreakmedia

Foreword

When I first introduced the Age Appropriate Design Code (AADC) into the Data Protection Bill in 2018, I had no idea that it may not apply to education settings. Now, a few years on, there is still some confusion. What happens if schools are working remotely: does the AADC suddenly apply? Or if a teacher uses an app or service in the classroom that they downloaded directly from the internet: does the AADC no longer apply? Why is there a difference between state and private schools, when surely all pupils need their data protected? Why is the burden disproportionately put on teachers and schools to understand the complex data processing terms set out in the terms and conditions of services that are hungry for data? And, perhaps most crucially of all, why are schools sharing intimate pupil data (wittingly and not) with commercial companies at all?

This report, authored by Emma Day, starts the work of unravelling some of these questions, and in doing so identifies gaps in provision, gaps in clarity, gaps in understanding. As such, it is the first step to working out what good might look like when the education sector and schools are brought into an effective data protection regime.

Our decision to work on education data preceded the pandemic that has shown just how urgent it is that government acts. The pandemic required emergency provision of remote learning, but it also supercharged the centrality of Google Classroom and Microsoft Teams in our schools. This normalised the use of a wide variety of EdTech without any corresponding protections, either in the proposed Online Safety Bill, or by formally extending the AADC so its application is beyond doubt.

The report owes a huge debt to defendigitalme who in 2020 published a detailed analysis of what was happening to pupil data. We salute them for their persistence in bringing this issue to the fore. While this report examines the regulatory questions and regime failure, it is important to keep in mind what is at stake. Data includes anything from intimate details of a medical visit made to the school nurse or assumptions about the child's aptitude or behaviour to how many clicks per minute pupils are doing in any particular lesson – and everything in between. Sharing this data, without adequate protection, leaves it open to abuse, discrimination, misinterpretation, commercial exploitation. And, if interpreted or used poorly, this can profoundly impact on a child's life chances.

There is undoubtedly, a positive role for data analytics to promote education, to support school administration, to make learning more fun or more styled to a particular pupil – or simply for research. But all those benefits rely on creating a data protection system applicable across the sector that is fair, trusted and understood. The DFC under the leadership of Professor Sonia Livingstone OBE is starting on the journey of describing what that system could be. We hope that this analysis of existing regulatory systems is a useful start.

– Baroness Beeban Kidron OBE

Beneficial uses of education data

This report marks the first step in the Digital Futures Commission's work stream on beneficial uses of education data. The aim is to explore current uses of student data in education settings so as to set out a child rights-respecting framework for data governance and practice. We have been hearing stakeholder concerns regarding the huge amounts of data being collected from children at school, with rising fears of data misuse, exploitation, surveillance and bias. We are also finding that schools, along with students and parents or caregivers, struggle to make informed choices in practice, lacking sufficient say regarding the use of children's data for learning, and as part of the commercial EdTech ecosystem.

The governance of data for children's learning in the UK state schools reveals significant regulatory and implementation gaps in data processing in education contexts. Emma Day's legal analysis of applicable governance frameworks, complemented by expert interviews, demonstrates the lack of enforceable guidance for translating existing legal requirements into practice for different types of data controllers and processors. She also documents the blurred responsibilities between schools and EdTech providers. This undermines schools', parents' or caregivers' and children's control and autonomy over the data generated and processed during teaching and learning.

Without meeting the challenges of education data governance, it is hard to build enthusiasm for unlocking the potential of education data, for this requires a trusted and effective governance regime. It will also require public deliberation over the educational and other benefits on offer, including consultation with children and young people, and robust research that weighs and evaluates the outcomes linked with different data uses. With this report, we offer an urgent analysis of the current governance landscape in UK state schools, identifying what regulation exists, the gaps or problems, and making practical recommendations for improvements in children's best interests.

- Professor Sonia Livingstone OBE

Author biography: Emma Day

Emma Day is a human rights lawyer specialising in children's rights and technology. Emma has spent the last twenty years working for a number of NGOs and UN agencies on a range of human rights issues and has lived in Eastern Africa, Southeast Asia, Canada and the UK. She is a non-practising solicitor and barrister (British Columbia 2010) and holds an LLM in International Human Rights Law from the University of London (2006) and an LLM in Law & Technology from the University of California, Berkeley (2020). Emma is an Affiliate at the Berkman Klein Center for Internet & Society, a non-resident Fellow at Atlantic Council's Digital Forensics Lab, and an Edmund Hillary Fellow.

Acknowledgements

This report benefited from significant input from the Digital Futures Commission (DFC) Commissioners, and from extensive reviews and comments from the DFC team led by Sonia Livingstone and including Kruakae Pothong and Ayça Atabey, and with specialised legal support from expert privacy lawyer, Laura Berton. Our findings and recommendations build on the systematic research into the EdTech sector by Jen Persson at defenddigitalme. Thanks also go to Baroness Beeban Kidron for her input and the team at the 5Rights Foundation for their support.

Glossary and acronyms

AADC	Age Appropriate Design Code
BESA	British Educational Suppliers Association
CoE	Council of Europe
CRIA	Child Rights Impact Assessment
DEA 2017	Digital Economy Act 2017
defenddigitalme	UK organisation that advocates for children's data and privacy rights in education
DfE	Department for Education
DfE Toolkit	Department for Education's Data Protection Toolkit for Schools
DPA 2018	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
EA 2010	Equality Act 2010
EDPB	European Data Protection Board
EdTech	Education technology
EEF	Education Endowment Fund
EU GDPR	The full text of the EU General Data Protection Regulation as it applies throughout the European Union (does not apply to the UK post Brexit, but the UK GDPR applies instead)
HRA 1998	Human Rights Act 1998
ICCPR	International Covenant on Civil and Political Rights
ICO	Information Commissioner's Office
ILRs	Individual Learner Records
Learning EdTech	Education technology used for teaching and learning (as defined by the Digital Futures Commission)
MAT	Multi-Academy Trust
NPD	National Pupil Database
National School Data	Data mandated to be collected termly from children in UK state schools via the school census under s537 of the Education Act 1996 (as defined by the Digital Futures Commission)
Ofqual	Office of Qualifications and Examinations Regulation
Ofsted	Office for Standards in Education, Children's Services and Skills
ONS	Office for National Statistics
PLR	Personal Learning Record
UK GDPR	The UK version of the GDPR as amended by the Keeling Schedule following Brexit
UNCRC	United Nations Convention on the Rights of the Child
ULN	Unique Learning Number
UPN	Unique Pupil Number

Executive summary 8
Part 1: The processing of children's education data 9
Scope and methodology 9
The education data landscape in UK schools 10
What is personal data and how does it relate to 'education data'? 10
What is the significance of 'education data'? 11
Why should children's education data be protected? 14
What types of 'education data' are processed in schools? 15
Legal protection for children's education data in the UK 17
Data protection regulations 17
The Five Safes framework 19
Purposes of the data processing 21
Part 2: The data governance framework – problems and recommendations 22
The role of government 22
Exemptions to the Five Safes framework 25
Legal issues for processing children's education data to support their learning 25
Applying the UK GDPR to education data 26
Data Protection Impact Assessment 26
Identifying the data controller and the data processor 27
Choosing a lawful basis for processing children's education data 30
Conclusion on data controllers and lawful basis in relation to Learning EdTech 31
The school as data controller for Learning EdTech 32
Education data processing on the lawful basis of public task 32
Special category data 32
What does the public task of education include? 32
Profiling and automated decision-making by Learning EdTech 35
Can Learning EdTech process data on the lawful basis of public task? 36
Procurement of Learning EdTech by schools 37
Government procurement and funding of Learning EdTech since COVID-19 38
Oversight of Learning EdTech compliance with data protection laws 40
The Learning EdTech company as independent data controller 42
When does the lawful basis of 'contract' apply? 42
When does the lawful basis of 'legitimate interests' apply to Learning EdTech? 42
The UK as a global EdTech marketplace 44
Part 3: The way forward 46
References 49

Executive summary

There is a growing reliance on education technology (EdTech) to deliver many aspects of school education and to further government and commercial interests in education-related data sharing. This growth in schools' EdTech usage, accelerated by the COVID-19 pandemic, opens up opportunities for data from and about children to be processed for commercial reasons as well as for educational and other purposes, some of them in the public interest. At the same time, we are witnessing uncertainties around education data governance that complicate the risk–benefit calculations to be made by stakeholders and can be linked to a lack of trust in both public and private sector management of children's education data.

This report provides a critical analysis of the current UK landscape for the governance of children's education data, focusing on EdTech used for teaching and learning in state schools. The analysis reveals significant regulatory and implementation gaps, and highlights legal and practical challenges for schools, regulators, EdTech businesses and families. The absence of a regulatory benchmark for what good (rights-respecting) data processing looks like in education contexts leaves both schools and EdTech companies with unclear responsibilities. These regulatory uncertainties complicate schools' data protection due diligence regarding EdTech decision-making and enforcement of contracts with service providers. Schools have few mechanisms and insufficient technical expertise or human resources to hold providers of EdTech companies accountable for the processing of children's data and its outcomes. EdTech providers have considerable latitude in interpreting the law and accessing children in real-time learning to test and develop their products.

This report unpacks these uncertainties regarding data governance as a key contribution to the Digital Futures Commission's aim of unlocking the beneficial uses of education data while mitigating the negative consequences of data exploitation. It identifies potential governance and oversight options for discussion. These concern EdTech procurement rules for schools, legally binding (EdTech) sector-specific guidance, and codes of practice and standards. In addition, potential governance mechanisms that could encourage the sharing of education data in the public interest are proposed for further exploration, such as mandatory data sharing by Learning EdTech companies with Department for Education (DfE), the creation of government-managed data trusts, and increased public data literacy.

The UK aims to be a leader in the global EdTech marketplace, competing with countries where children's data rights are becomingly increasingly significant to governments. The report concludes by suggesting that promotion of and compliance with the highest international standards on data protection and child rights makes good business sense as well as being the right thing to do for children in the UK.

Part 1: The processing of children's education data

School is the one environment that children up to the age of 16 are mandated by law to attend, unless their parents or caregivers formally opt to educate them in an alternative environment.[1] While at school, data about children are processed for various purposes, including administration, resource allocation, marketing, safety, and improvement of teaching, learning, attendance and assessment. All of these can be described as education data, being processed at, by or in relation to the school's activities, although not all necessarily serve educational purposes. The governance of these different kinds of data encompasses a myriad of different laws and policies.

Scope and methodology

In the interests of bringing clarity to a complicated data landscape, this report examines the governance of personal data processed from children in state schools in the UK *for the purposes of teaching and learning*.[2] This encompasses the National School Data processed by the DfE and the use of EdTech by schools (as further explained below).

Note that other forms of education data, including administrative data, such as data processed to administer school meals (Department for Education, 2018d),[3] school trips and school marketing, as well as data processed by safety technologies (such as monitoring and filtering of children's internet searches and communications) are beyond the scope of this report because they come under different governance frameworks, with different permitted lawful bases for processing children's education data (as explained below).[4]

This report primarily involved desk research into the data governance landscape related to EdTech in the UK, including laws, policies, government strategy papers and private sector policy papers. Grey literature related to data governance and children was also reviewed. To supplement this desk research, interviews were carried out with various

[1] This report concerns children aged 4–16 because these are the mandatory years for attending school in the UK. The permitted school leaving age is 16 throughout the UK, but children leaving school at 16 in England must either stay in education, start a traineeship, or pursue part-time education until 18.

[2] In this report, "state schools" refers to UK state funded schools. We focus on state schools because of their status as public authorities which subjects them to enhanced government oversight and entails certain obligations prescribed by the UK GDPR that private schools are exempt from. Though the UK GDPR applies to all schools, private schools are not obliged by the UK GDPR to appoint a data protection officer (DPO). Nor are private schools obliged to respond to pupils' data subject requests to access information under the Freedom of Information Act.

[3] There has been controversy surrounding schools' processing of children's biometric identification as proof of payment for school meals. Although currently lawful in the UK, collecting biometric data from children comes under the Protection of Freedoms Act 2012.

[4] However, it is noted that this may be a somewhat artificial division in that the same company may provide EdTech that is used for multiple purposes. Where this is the case, it would be necessary to carry out a separate analysis of each of the core and non-core purposes for data processing, and the same company may require a different lawful basis (Article 6, UK GDPR) for each.

experts in EdTech and children's data, including from the private sector, civil society and lawyers in private practice.

The education data landscape in UK schools

What is personal data and how does it relate to 'education data'?

Currently, any collection and processing of personal data, [5] including education data (as defined in this report) are regulated under the Data Protection Act (DPA) 2018 and the UK General Data Protection Regulation (GDPR).[6]

Personal data[7]

Personal data only includes information relating to 'natural persons' who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information. An individual is 'identifiable' if you can distinguish them from other individuals (Information Commissioner's Office, 2021b, p. 9).

Personal data may also include special categories[8] that are considered sensitive and so may only be processed in more limited circumstances (e.g., data related to health or sexuality).

Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.[9]

If personal data can be truly anonymised, then the anonymised data is not subject to the UK GDPR (Information Commissioner's Office, 2021b, p. 9).[10]

[5] Article 4(2) of the UK GDPR defines 'processing' as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' Aligned with the UK-GDPR definition, the Glossary for General Comment No.25 on Children's Rights in Relation to the Digital Environment provides that 'data processing' includes processes of data collection, recording, retention, analysis, dissemination and use (United Nations Committee on the Rights of the Child, 2021, p. 2).

[6] Because the definition of personal data is broad, it can be difficult to draw the line between 'personal' and 'non-personal' data (Purtova, 2018, p. 10). For example, it is difficult to find specific examples of children's data that would be considered non-personal.

[7] Paraphrased and adapted from 'What is personal data?' (Information Commissioner's Office, 2021b, p.9). Recital 26 of the UK GDPR provides that the UK GDPR does not apply to anonymous data.

[8] Article 9 of the UK GDPR. Refer to the section on special category data on p.34.

[9] Recital 26 makes it clear that pseudonymised personal data remains personal data.

[10] It has been argued that perfect anonymisation is becoming impossible, and it must therefore always be taken into account that there is some risk of re-identification of individuals, especially as data are stored into the future and technology continues to advance exponentially. (Narayanan & Shmatikov, 2010, p. 26; The Article 29 Data Protection Working Party, 2013, p. 31) Relatedly, as technology has developed, the increasing availability of data analysis algorithms and sophisticated hardware has made it easier to link data sets and infer personal information from data that may appear to be non-personal (Finck & Pallas, 2020, p. 20; Ohm, 2010, p. 1731).

Personal data relevant to schools includes any personally identifiable data processed from children either by the school or by a processor instructed or permitted by the schools to process children's data. This notion of personal data relevant to schools forms our scope and definition of 'education data', extending the definition of 'education data' in the DPA 2018[11]. The DPA 2018 definition is limited to personal data that forms part of an educational record, excluding health data (Information Commissioner's Office, 2020g, p. 67). We recognise that some EdTech companies may process data related to children's mental health or special educational needs. Thus, our definition of 'education data' includes health data processed from children and other data sets processed by EdTech companies[12] even though some of these may not form part of the child's educational record.

'Education data'

Our definition of 'education data' refers to personally identifiable information processed from children within a specific context of state schools, either by the schools themselves or data processors authorised by schools.

Education data is currently processed by three main entities: the national government (specifically, the DfE and the Office for National Statistics (ONS), which maintain the National Pupil Database (NPD) and Individual Learner Records (ILRs) for children), schools and EdTech companies. Schools that are mandated by law to process children's education data and provide it to the DfE. Schools also process children's data as a part of teaching and assessment, to enable school administration and to fulfil their duty under the law.[13] EdTech companies also process children's education data, as is examined in what follows.

What is the significance of 'education data'?

Data have always been processed from children in schools, and some data processing is necessary for the school's functioning and to monitor the educational development of individual children. There is also value in making aggregated education data available to researchers who can contribute to evidence-based policy and use data to create learning technology tools and improve learning outcomes for children. The main value of data is not in their raw format but in their processing into algorithms that allow predictive value to be extracted from them (Komljenovic, 2021, p. 6). In the education context, personalised and tailored teaching and learning processes are particularly valuable (Komljenovic, 2021, p. 6).[14]

[11] DPA 2018, Schedule 3, Part 4, paras 13–17.

[12] Refer to the types of data processed by EdTech providers on pp. 15-16.

[13] In addition to the key legislation that constitutes mandatory data processing by schools to be shared with DfE, other pieces of legislation, including the Education Act 1996, the Counter-Terrorism and Security Act 2015 and the Prevent Duty Guidance (UK Home Office, 2021) also result in education data being processed for the purposes of preventing terrorism. Education data is also processed by EdTech companies contracted by schools to support teaching and learning, as a tool for school administration or for the purposes of safety and security.

[14] Once the predictive value has been extracted from data sets, from a commercial perspective they could be destroyed by EdTech companies relatively quickly after the algorithm has been developed. This could be good risk management due to the vulnerability of anonymised data sets to re-identification by persistent hackers. However, there are also reasons to retain the underlying data that were used to train any algorithm, because when algorithms lead to unfair or harmful outcomes, researchers and policymakers need to be able to review the underlying data sets to understand how they were

It has been a legal requirement for schools to provide National School Data to the DfE since the Education Act came into force in 1996 (Section 537A). The school census is carried out three times a year in the UK and is mandatory for all state schools (Department for Education, 2019b).

National School Data

Data are mandated to be collected termly from children in state schools via the school census under Section 537 of the Education Act 1996. We refer to these as 'National School Data'. These data are used to calculate schools' per capita allocation of funding (Department for Education, 2019b). Schools are mandated to allocate Unique Pupil Numbers (UPNs) to all students when they first enrol in a state school under Section 537A of the Education Act 1996 and to provide this information to the local authority and the DfE. The UPN stays with the child for life. Schools are also required to allocate each child a Unique Learning Number (ULN), which is used as a key identifier for their Personal Learning Record, including the child's full personal data, verified qualifications and a record of what they have studied and achieved since the age of 14 (Education and Skills Funding Agency, 2018). Schools are legally entitled to transfer these data to subsequent schools attended by the child (Education Act 1996, Section 408) without prior consent from the child or their parents or caregivers (Department for Education, 2019e, p. 10).[15]

The DfE and the ONS manage National School Data, and researchers can access these databases to inform policy and practice. They may also be accessed by private companies developing EdTech tools. Access to these data is governed by the Digital Economy Act (DEA) 2017, the DPA 2018 and the UK GDPR.[16] The schools and DfE act as either independent or joint data controllers for this database under the UK GDPR, depending on the circumstances, as they are both mandated by law to process defined categories of education data from schools.

In recent years, the amount of education data processed from children in the UK has grown exponentially (see Figure 1). The English national data landscape was mapped comprehensively in 2020 by defenddigitalme, a UK organisation that advocates for children's data and privacy rights in education (Persson, 2020). This revealed the scale

trained and to ensure the same mistakes are not repeated. The ability to retrospectively audit training data sets is particularly important when algorithms are used in the public sector, due to the tendency of algorithms to perpetuate patterns of inequality contained in the training data. This was illustrated in the algorithm developed by the Office of Qualifications and Examinations Regulation (Ofqual) to predict exam results by postcode in the summer of 2020 (Coughlan, 2020).

[15] Before 2002, the annual school census only included aggregated data for the school as a whole and not information about individuals. Since 2002 termly data collections have included individual pupil names. Only three out of around 400 possible submitted data points on each child are optional across the census, including country of birth, nationality, ethnicity, service family child and adopted from care (Persson, 2020).

[16] The DEA 2017 aims to 'improve public services through the better use of data while ensuring privacy, clarity and consistency in how the public sector shares data' (Information Commissioner's Office, 2020a, p. 66). It covers education data, but not data sharing relating to the provision of health and social care. By default, all education data shared with data processors from education data sets must be done through the ONS Secure Research Service (SRS), managed by the DfE and the ONS. Exemptions are allowed by application to the DfE to access education data directly (not via the SRS) on the grounds that: data are being processed to fulfil an essential public task, such as the running of education or children's services; for research funded by or commissioned by the DfE and its executive agencies or other government departments; or for research sponsored by the DfE.

of data processing from children in schools and the high degree of onward sharing and reuse of those data. his is partly because the categories of data mandated to be processed by schools have increased significantly, both in quantity and scope, since the Education Act 1996, not without controversy in relation to the parameters of education data (defenddigitalme, 2018).[17] Before 2002, the annual school census only included aggregated data for the school as a whole and not information about individuals (Persson, 2020). By 2020, this had changed considerably.[18]

Also noteworthy is that, until recently, the only way to access children's education data at a national level was by application to the DfE and/or ONS following the UK Statistics Authority (2020) Research Code of Practice and Accreditation Criteria (Code of Practice).[19] That was until EdTech companies started to contract directly with schools to deliver services to teachers and pupils, and they are thereby now able to process children's education data directly. The scale of education data processing by EdTech companies has further increased massively since the COVID-19 pandemic forced UK schools online for extended periods, while the EdTech sector grew by 72% in 2020 (Walters, 2021). Google reported in May 2021 that their user numbers for Google Classroom rose to 150 million from 40 million the previous year (Williamson, 2021).

[17] For example, in 2021, following a compulsory audit of the DfE by the ICO, children's country of birth and nationality data was deleted from the DfE database because the ICO found this was being shared with the Home Office, which was beyond the scope of its original educational purpose and in breach of data protection laws.

[18] The expansion in scope and scale of data processed from children in state schools results mainly from gradual successive secondary legislation, including the Education (School Performance Information) (England) Regulations 2007, SI 2007/2324), Education (Individual Pupil Information) (Prescribed Persons) (England) Regulations 2009, SI 2009/1563, Small Business, Enterprise and Employment Act 2015. These gradual legislative changes have not only increased the amount and variety of named data being collected and shared between schools, the DfE and local authorities, but also enabled linkage of NPD, HE, FE with datasets to create the "destinations data" and Longitudinal Educational Outcomes (LEO) (Persson, 2020).

[19] Refer to p. 20 of this report.

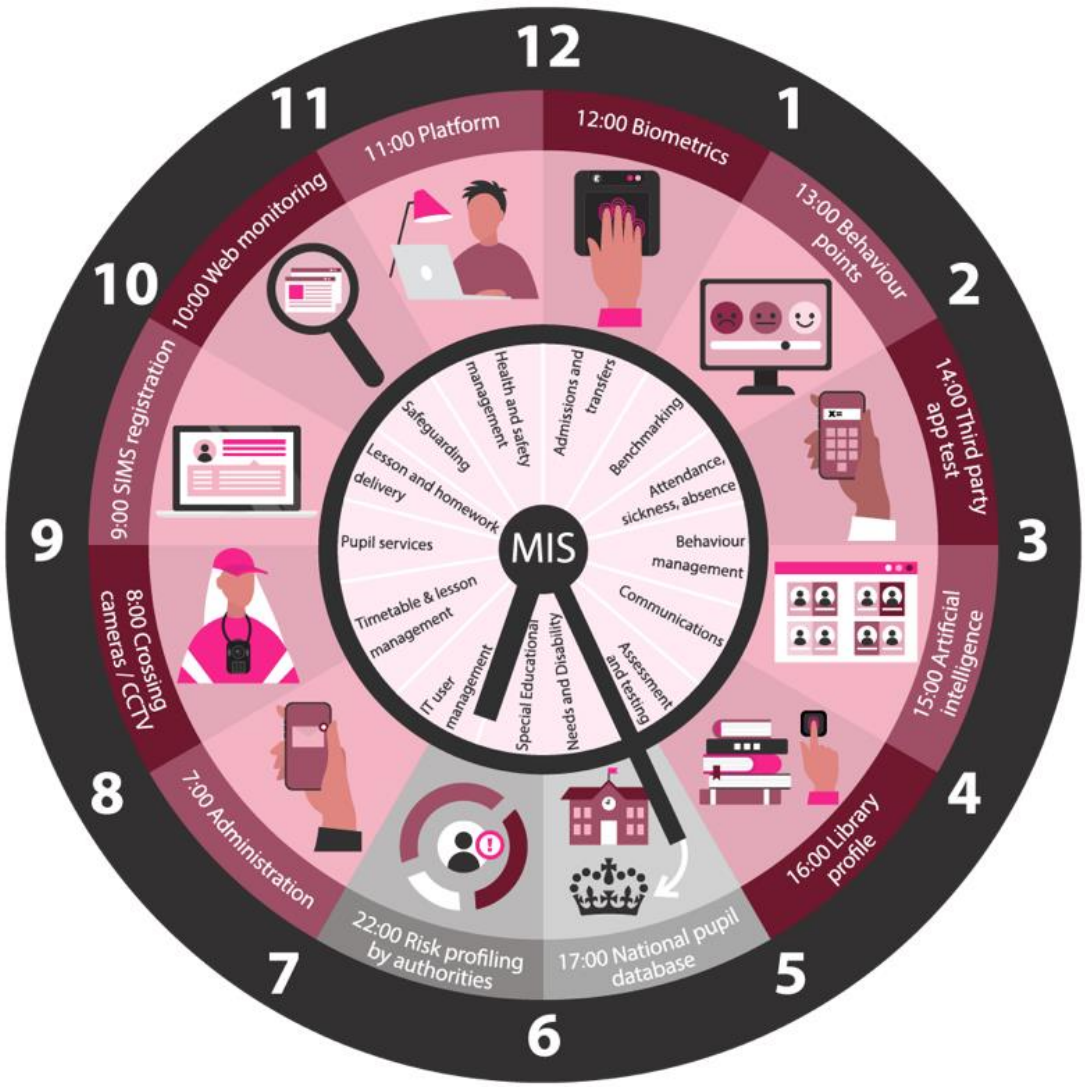

Figure 1. An illustration of a day in life of an eleven-year-old girl at a state secondary school in the UK, as captured in *The State of Data 2020* (Persson, 2020)

Why should children's education data be protected?

Children are a recognised vulnerable group[20] under the UK GDPR. Education data can reveal particularly sensitive and protected characteristics about children, such as their ethnicity, religion, disability or health status (Data Protection in Schools, n.d.; National Center for Education Statistics, 2016). Education data can also be used to create algorithms that profile children and predict or assess their academic ability and performance (Kurni & Srinivasa, 2021, p. 5). Childhood is an important time for the

[20] Note that children are the only vulnerable group specified under Recital 75 of the UK GDPR: '[…] vulnerable natural persons, in particular of children […]'. Recital 38 of the UK GDPR states that 'Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.'

development of identity and personality, and children need to be free to experiment with this. There is a risk that profiling of children using their data can lead to deterministic outcomes such as defining early on what subjects the child is good at or not, how creative they are, and what they are interested in. Safeguards must be put in place in relation to the processing of children's personal data in schools to protect their fundamental rights.

Children have the right to education under the United Nations Convention on the Rights of the Child (UNCRC) 1989 and the Human Rights Act (HRA) 1998, but they also have rights to privacy and freedom of thought, and all of these and other rights must be balanced against each other. Recital 4 to the EU GDPR (although not binding in the UK) states that the right to protection of personal data is not an absolute right but must be considered in relation to its 'function in society' and be balanced against other fundamental rights, in accordance with the principle of proportionality.[21] On first review, the case for either risks or benefits is still contested and requires further research, although that was not the primary focus of this report. Further phases of this research will involve a more thorough review of the state of the evidence of both the educational benefits of EdTech and of the potential child rights harms (including in relation to data). It is difficult to carry out a proportionality assessment based on theoretical risks and benefits.

Children's rights: duty bearers and rights holders

Taking a child-rights based approach, children in the UK have rights under the UNCRC 1989, the International Covenant on Civil and Political Rights (ICCPR) 1966, the HRA 1998, the DPA 2018 and the UK GDPR, as well as many others. The UNCRC sets out children's rights at an international level, including their rights to education, privacy, play and participation. In 2021, the UN Committee on the Rights of the Child (2021) set out in their General Comment No. 25 how all of the rights in the UNCRC apply in the digital environment. The state is the principal duty bearer for these rights, which means the government is responsible for protecting, respecting and fulfilling children's rights at a national level. All state actors hold this responsibility, which means that teachers, social workers, civil servants and police officers are all duty bearers. Children are rights holders, which means that they have the right to exercise their rights, hold duty bearers accountable and seek redress.

What types of 'education data' are processed in schools?

Education data is processed from children under four parallel areas of law, the first three of which relate to schools:

1. Data processed by schools are shared with the DfE, which manages the NPD and ILRs (Department for Education, 2018c). These data are processed pursuant to the Education Act 1996 and in line with the DPA 2018, the UK GDPR, the HRA 1998 and the Equality Act (EA) 2010. Because the DfE is a public authority, access to these data comes under the DEA 2017 ('National School Data').

[21] Note that because the EU Charter of Fundamental Rights no longer forms a part of retained EU law in the UK post Brexit, the reference to fundamental rights may not be relevant to the interpretation of the UK GDPR. However, children still have rights under the HRA 1998 and the UNCRC, which need to be factored into this balancing of rights.

2. EdTech companies process children's data when they contract[22] with schools to provide services for:

    a. information management ('Management EdTech');

    b. education and learning platforms, and technology tools to support learning and assessment ('Learning EdTech').

    This education data comes under the UK GDPR, the DPA 2018, the HRA 1998 and the EA 2010, and sometimes the Age Appropriate Design Code (AADC) (depending on the context[23]), but not the DEA 2017.

3. Safety technology companies (also categorised as 'EdTech' under the national EdTech Strategy (Department for Education, 2019d, p. 23) process data from children when they contract with schools to provide services for monitoring and filtering children's online activities. These data come under the UK GDPR, the DPA 2018, the HRA 1998 and the EA 2010, the Counter-Terrorism and Security Act 2015, and related Prevent Duty Guidance for England and Wales (UK Home Office, 2021), as well as the AADC ('Safety EdTech').

4. Data processed by EdTech companies directly from children outside of schools are regulated by the UK GDPR, the DPA 2018, the HRA 1998 and the EA 2010, as well as the AADC[24] ('Home EdTech').

This report focuses on categories 1 (National School Data) and 2(b) (data generated from uses of Learning EdTech) which include the data illustrated in Table 1.[25]

National School Data	• First name, • Last name, • Middle name(s), • Former names, • Date of Birth, Gender, • Ethnicity, First language, • Special Educational Needs and Disability, • Home address, Unique Pupil Number (UPN) 0+, • Unique Learner Number (ULN) 14+, • Any form of UPN processed from children through schools' usage of information management systems, such as Capita Sims. *Note: This list derives from The State of Data 2020 (Persson, 2020, p. 28)*

[22] Even where companies provide Learning EdTech products for free, the school must enter into an agreement with the company, which is legally binding on both parties.

[23] Refer to the summary of the AADC on p.19.

[24] The Information Commissioner's Office (ICO) has determined that 'If an ISS is only offered through an intermediary, such as a school, then it is not offered "directly" to a child.' (Information Commissioner's Office, 2018, p. 24)

[25] We note that, in practice, Learning EdTech processes both the data that form the National School Data and the data processed from children by EdTech providers, as part of their information management and learning (including assessment) services to schools (see the first two categories of our education data).

Data generated from the use of learning EdTech	• Lesson & homework delivery generated, for example from the use of an information society service such as Show My Homework[26]. • Health data (from health & safety management) • Online learning, including engagement and usage data, attendance and absence and resulting metadata (e.g., IP address, device information, including hardware model, operating system version, unique device identifiers, mobile network information and phone number) generated, for example from the use of Google Classroom[27] or HegartyMaths[28]) • Assessment and testing results *Note: This list is indicative, and is based on existing research (Persson, 2020) and additional research by the DFC in its Guidance for Innovators work stream*

Table 1: Summary of data processed under the two categories of education data focussed on in this report.

The rationale is that the use of technology for teaching and learning goes to the heart of children's educational experience and can fundamentally change both the content of what they learn and the underpinning pedagogy. In addition, the private sector has now taken on a significant role in delivering children's education in state schools, thereby giving companies access to real-time personal data directly from children and an unprecedented influence over the substance of their lessons and how they are taught. There is therefore a need to reflect on the degree to which law and policy have kept up with these changes and the extent to which the government, as overall duty bearer, has maintained oversight and control.

Legal protection for children's education data in the UK

Data protection regulations

The DPA 2018 sets out the framework for data protection law in the UK, and it sits alongside and supplements the UK GDPR which sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies. The UK GDPR is the most applicable law to this analysis of education data governance in the UK. The ICO is the UK's independent authority responsible for upholding data subjects' (including children's) information rights, designated by the DPA.

The UK GDPR is underpinned by the following principles (Article 5):

- *Lawfulness, fairness and transparency* – schools and EdTech companies must have a lawful basis for processing education data, and ensure that processing is lawful in

[26] Derived from Show-my-homework privacy policy. (Show My Homework, n.d.)

[27] Derived from Google Classroom notice to parents and guardians of children attending Ridgeway Primary Academy. (Ridgeway Primary Academy, n.d.)

[28] Derived from privacy notice for schools using Hegartymaths. (HegartyMaths, 2020)

a general sense. They must process data in a way that is fair, clear, open and honest,

- *Purpose limitation* - schools and EdTech companies must be clear about the purposes for which they are collecting data and not use the data for any other purpose in the future without permission
- *Data minimisation* - schools and EdTech companies must only collect the data that are adequate to fulfil their stated purpose, relevant to that purpose, and limited to what is necessary.
- *Accuracy* – schools and EdTech companies should ensure the data they process are accurate and keep it updated
- *Storage limitation* – education data must not be kept for longer than it is needed
- *Security* – there must be appropriate security measures in place to protect the integrity and confidentiality of the data
- *Accountability* – schools and EdTech companies must take responsibility for what they do with education data and how they comply with the UK GDPR principles.

What is the Information Commissioner's Office?

The ICO is the UK's independent data protection authority whose role is to uphold information rights in the public interest:

- The ICO provides guidance on legislation, as well as statutory codes such as the AADC. The ICO covers the DPA 2018, the Freedom of Information Act 2000, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the UK GDPR and the Reuse of Public Sector Information Regulations 2015, among others.
- Schools are mandated under the DPA 2018 to appoint a data protection officer and register them with the ICO. The ICO can carry out audits on the request of a school or choose to impose mandatory audits on schools. In 2018–19 the ICO carried out a consensual audit of 11 Multi-Academy Trusts' (MATs) processing of education data and other personal data in 325 schools (Information Commissioner's Office, 2020b). The outcome of the ICO audits were published on their website in 2020.
- Children's parents or caregivers can complain to the ICO if they believe their data have been mishandled by their school or by an EdTech company. The ICO has the power to investigate complaints and to issue an enforcement notice if they find a school or an EdTech company has failed to comply with data protection laws.
- The ICO can also investigate specific sectors, as it did, for example, in 2018 when it investigated the data broking sector and consequently issued an enforcement action against the credit reference agency Experian Limited (Information Commissioner's Office, 2020e; 2020f, pp. 36-37). It would be within the ICO's mandate to launch a similar investigation into the EdTech sector.

The UK GDPR also sets out the legal bases under which personal data including education data can be processed, and the individual rights of the data subjects, who are the children whose data are being processed. Children (like adults) have rights to: be informed about data being processed from them; to access that data, to rectify the data record, to erasure; to restrict processing; to data portability; to object; and rights related to automated decision-making including profiling (Information Commissioner's Office, 2018, p. 40).

What Is the Age Appropriate Design Code (AADC)?

The AADC is a statutory code produced by the ICO pursuant to section 123(1) of the DPA 2018. The AADC draws on the UNCRC and helps companies apply the UK GDPR in a child rights-respecting manner. It is a code of practice on age-appropriate design of relevant information society services that are ***likely to be accessed by children*** (Information Commissioner's Office, 2020a, p. 9). The DPA 2018 provides that courts and tribunals must take into account the provisions of the AADC where relevant to the proceedings in question (Department for Digital Culture Media & Sport, 2020). This means that the AADC can be used to interpret the law wherever the UK GDPR and the DPA 2018 apply. The AADC introduces risk-based age assurance and prevents services from nudging children to lower their privacy settings or provide unnecessary personal data.[29] It provides that the best interests of the child must be a primary consideration when companies design and develop online services likely to be accessed by a child, and advises that a Data Protection Impact Assessment (DPIA) should be carried out (Information Commissioner's Office, 2020a, pp. 27-31; 2021h).[30] The AADC is not a law itself. It is referred to in the DPA 2018 and is a form of statutory guidance

In addition to the DPA 2018, data collected from children in state schools by the school census under Section 537 of the Education Act 1996 are protected by the Five Safes Framework, developed by the ONS.

The Five Safes framework

For research carried out using DfE data, there is a statutory duty under Chapter 5 of the DEA 2017 for research project accreditation according to the UK Statistics Authority Research Code of Practice and Accreditation Criteria (Code of Practice) (UK Statistics Authority, 2020). The application for research must go through initial feasibility and public good checks by the ONS Statistical Support team, and data owner approval is sought (UK Statistics Authority, 2019b). The proposal must also go before an ethics review board and the ONS review board.

Applicants wishing to access DfE data through the Office for National Statistics Secure Research Service (SRS) (Department for Education, 2018b) must evidence that they comply with the Fives Safes framework, which relates to safe people, safe projects, safe settings, safe outputs and safe data. The ONS developed the Five Safes framework in 2003 to balance user requests to access data with ethical considerations.

In the absence of any other similar framework, it has become a commonly used standard for addressing data access solutions by the UK, Germany, the US and some international bodies (Ritchie, 2017, p. 1).

[29] The AADC sets out 15 standards that build in a high bar of data protection to digital products and services that are likely to be accessed by children. For example, by applying the 15 standards, the AADC ensures that children's profiles are 'private' by default, their locations are not tracked or made visible, and their data are not shared with data processors outside of a contract or used to recommend content that is injurious to their wellbeing.

[30] Article 35(4) of the GDPR requires the ICO list of processing operations that are likely to result in high risk and therefore require a DPIA. This list includes '9. Targeting of children or other vulnerable individuals: the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.'

i. Safe people

The first of the Five Safes requires that individuals accessing children's education data are 'safe people'. This is because education data includes highly sensitive and personably identifiable information related to children, who are already a vulnerable group of data subjects. These data could be used to inform assessments made about children's learning, abilities, and behaviour. However, these data could also be used by predators to identify and locate vulnerable children. Therefore, anyone analysing children's data should be properly accredited and meet a number of requirements.

To apply to access DfE data through the SRS, in accordance with the first of the Five Safes, the applicant must be accredited under the ONS approved researcher scheme. The Code of Practice (UK Statistics Authority, 2020) sets out requirements for researchers accessing public data sets such as DfE data, pursuant to Section 70(1) of the DEA 2017. The Code of Practice mandates researchers to provide a criminal record check, and a record of appropriate compliance with UK laws, in particular, those relevant to the use of data (UK Statistics Authority, 2020). Since the COVID-19 pandemic, a special concession has been made to allow some researchers to access SRS data from home, but this is not an automatic extension for all (Office for National Statistics, 2020a).[31] Only suitably qualified and trained individuals are allowed access to the data. A complete list of accredited researchers is published on the UK Statistics Authority website to ensure transparent access, and accredited researchers must consent to be audited by them. The DEA 2017 (Section 64(10)) introduces new criminal offences where personal information is received under the research power and disclosed in breach of the Sections 66-69 of the Act (Office for National Statistics, 2020a).

ii. Safe projects

The potential for security breaches wherever children's data are stored is significant and a real risk. A breach of children's education data poses both a risk to the children involved and also potentially presents a risk to national security (Landau, 2018). Once data have been exposed, although it is possible to patch the security hole, it is not possible to retrieve the data from anyone who may have accessed it during the breach or prevent them from using it or sharing it onwards; therefore, the privacy breach is irrevocable. This is one reason why the data minimisation principle[32] is important, because the best way to protect children's privacy is to process and store less of their data.

In principle, the ONS SRS provides the highest level of security in relation to children's education data, and there are strict cybersecurity measures included in the regulatory framework related to the DfE database. Access to DfE data via the ONS SRS is only possible using their secure technology systems (Office for National Statistics, 2020c),

[31] Approved researchers must have an undergraduate degree, including a significant element of maths or stats, or at least three years of quantitative research experience, plus completion of a safe researcher training course (UK Statistics Authority, 2019a, p. 1). Researchers who do not have the required training and experience can apply to be a provisional accredited researcher, but must be supervised by a fully accredited researcher (Office for National Statistics, 2020a).

[32] Article 5(1)(c) of the UK GDPR provides that 'Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)'.

which gives the DfE direct oversight and control over the security measures in place to protect the data from security breaches.

iii. Safe settings

Access to DfE data is only possible using ONS secure technology systems. Most datasets are available through remote access to the SRS, but some can only be accessed in an approved safe setting. For researchers based overseas, any research must be undertaken within a UK-based secure environment accredited under the DEA 2017 (Office for National Statistics, 2020b; UK Statistics Authority, 2019a, p. 2).

iv. Safe outputs

All research outputs from the DfE database are checked to ensure they cannot identify data subjects (Office for National Statistics, 2020c).

v. Safe data

Under the Code of Practice (UK Statistics Authority, 2020), researchers accessing DfE data can only use data that has been de-identified (Office for National Statistics, 2020c).

Purposes of the data processing

The DEA 2017 makes it clear that public sector bodies should only share data when there is a clear public benefit. Data requested from the DfE must be for research in the public interest (UK Statistics Authority, 2019b, p. 2; 2020), which means the primary purpose of the research must be to:

- Provide an evidence base for public policy decision-making;
- Provide an evidence base for public service delivery;
- Provide an evidence base for decisions that are likely to significantly benefit the UK economy, society or quality of life of people in the UK;
- Replicate, validate or challenge official statistics;
- Replicate, validate or challenge existing research;
- Significantly extend understanding of social or economic trends or events by improving knowledge or challenging widely accepted analyses; or
- Improve the quality, coverage or presentation of existing statistical information.

Applicants are also required to provide full details of the research methodology, including any statistical methods, collaborative work or additional data sources to be used (linked data, web scraping, survey results etc.). Finally, the ethical consideration of the research project is assessed, and the final checked application is submitted to the Research Accreditation Panel for independent accreditation. In addition, to meet the criteria of a public good, research findings must usually be published

Part 2: The data governance framework – problems and recommendations

Against the backdrop of exponential growth of education data processing, described in Part 1, and in spite of the protections afforded by the DPA 2018, the UK GDPR, the DEA 2017, and the AADC, this report questions the government's control over education data governance, based on our deep dive into the data governance of Learning EdTech.

The role of government

Good governance and the rule of law require primary legislation to be laid down by Parliament and to be subject to debate. The government has not produced any legislation specifically concerning any kind of EdTech or education data, so there is no overarching 'education data' governance framework. Nor does there appear to be effective government oversight of Learning EdTech companies' compliance with data protection or cybersecurity laws and standards, or systematic audits of schools or EdTech companies.

The DfE offers a webpage of 'Guidance and support for education providers who want to increase their use of EdTech' (2019f) which directs schools to the EdTech Strategy and the Data Protection Toolkit for Schools (DfE Toolkit) (2018a). The DfE Toolkit was published in August 2018. The DfE Toolkit does not provide guidance on the legal bases on which data can be processed from children. Nor does it provide sufficient guidance for schools to decide whether they need to use Learning EdTech, to choose between EdTech companies, or to negotiate a contract with an EdTech company. Indeed, there appears to be no government procurement guidance for schools based on criteria related to the Learning EdTech tools that have been shown to improve children's learning outcomes.

The DfE Data Protection Toolkit for Schools (2018)

The DfE Toolkit outlines nine steps that the DfE thinks can help schools efficiently develop the culture, processes and documentation required to comply with the DPA 2018 and the UK GDPR. There is no specific reference to EdTech, and it is stressed that the DfE Toolkit 'provides tips and guidance only' and 'does not constitute formal legal guidance' (Department for Education, 2018a, p. 7). It includes the disclaimer that the school, as a data controller, is ultimately responsible for its data protection procedures and compliance with legislation, and that compliance is the responsibility of the governors and trustees of the school.

Multiple kinds of EdTech are included in the government's EdTech Strategy (Department for Education, 2019d), although only Learning EdTech is within the scope of this report.

The UK EdTech Strategy

In April 2019, the DfE published *Realising the potential of technology in education: A strategy for education providers and the technology industry* (Department for Education, 2019d). The Strategy's aims include, amongst other things: setting the DfE's vision for EdTech; supporting effective procurement of EdTech; and developing a dynamic EdTech

business sector that positions the UK as a world leader in EdTech. The EdTech Strategy is not a law or regulation, but is an aspirational discussion paper regarding the EdTech sector in the UK. It is the only government guidance related to EdTech in the UK.

It covers Management EdTech, Learning EdTech, Safety EdTech and Home EdTech, plus a section on promoting the EdTech sector globally as a UK business sector. The Strategy provides little specific guidance to schools, instead signposting the reader to the DPA 2018, the UK GDPR, generic data protection advice from the ICO not tailored to schools, and advice from a variety of websites from non-profit organisations and private consulting companies. Anecdotal quotes from schools recommending different EdTech products are interspersed throughout. The government assumes no responsibility for the advice of third parties that it signposts the reader to, and reminds the schools that they are the data controller and remain legally responsible for the education data they process.

While preparing this report, we interviewed a range of experts who gave contradictory views on the applicability of the AADC to Learning EdTech and schools. We note that the ICO has not provided specific guidance to schools on the applicability of the AADC, and we have learned of confusion regarding whether or not it applies to EdTech, as discussed below. There also appears to be confusion regarding when exactly a school is a data controller, a joint data controller or an independent data controller, and when a Learning EdTech company is a data processor or an independent data controller. We also discovered different understandings of whether or not EdTech companies can enter into contracts directly with children for optional extra add-on features and whether EdTech companies can directly advertise to children.

The responsibilities for dictating the use and purposes of data processing are split between EdTech companies and schools and there is a lack of clarity about which has primary responsibility in any given context. State schools are left to navigate generic data protection compliance guidance from the ICO, which do not directly address the special concerns they must consider as a public authority with legal responsibility for children, such as what is an educational purpose, and how the UK GDPR, the DPA 2018 and the AADC apply to Learning EdTech. Not only is each school data protection officer left to navigate this confusing landscape on a school-by-school basis, but there is little or no systematic government oversight of whether or not they are getting it right.

No wonder it has been argued that the UK education data and governance landscape is marked by four layers of complexity, linked to four types of problem (Persson, 2020); see Figure 2).

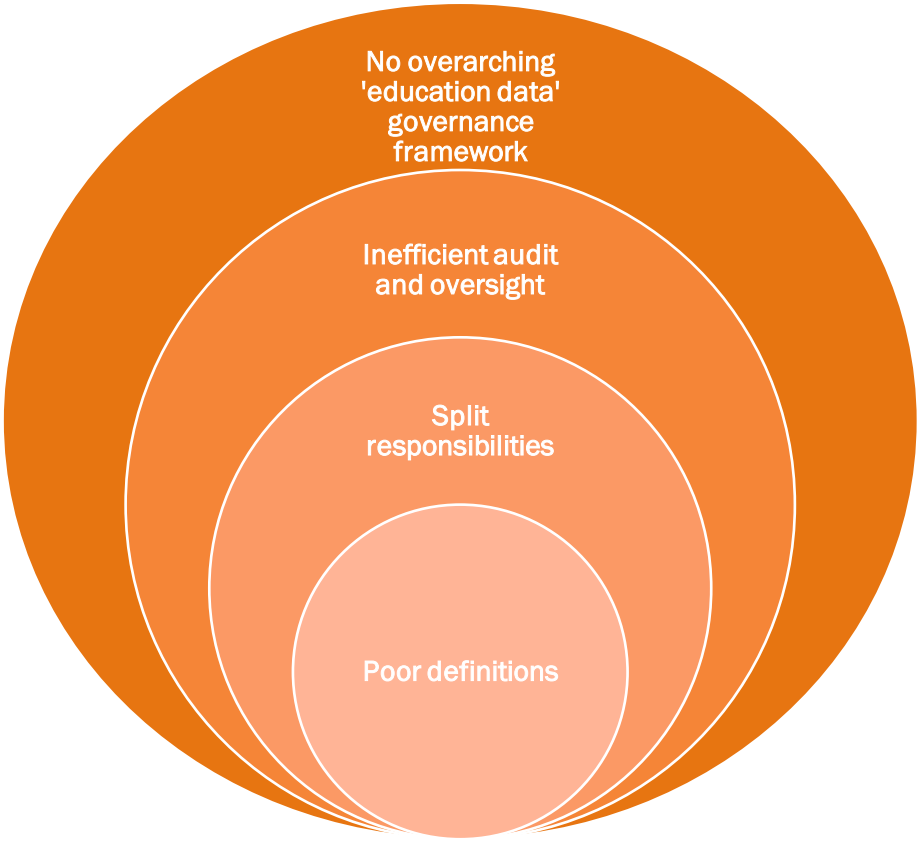

Figure 2: Statutory national assessment data collections, Persson 2020

As the primary duty bearer in relation to children's rights in general and their right to education in particular, the government appears to have delegated its duty to regulate in this area to the private sector and the non-profit sector, leaving itself seemingly unaccountable for the Learning EdTech sector that is rapidly becoming central to education in the UK. This leaves schools with a heavy responsibility to digest a confusing array of laws, policies and research reports and be solely accountable for their decisions in this regard.

It is the responsibility of the government as overall duty bearer and custodian of children's rights to come up with an effective governance framework – whether that be through new legislation, standards or some kind of an independent oversight mechanism – to ensure that EdTech products used in state schools are (i) independently evaluated; (ii) shown to produce credible improvements in teaching and learning; and (iii) comply with data protection regulations. This role is arguably on the same level of importance as determining the contents of the national curriculum.

Recommendation 1: The current governance framework is complicated, and the experts we interviewed found it to be confusing. There is need for ICO guidance that sets out how the UK GDPR and the DPA 2018 should apply to the education data processed by Learning EdTech companies in schools.

Exemptions to the Five Safes framework

Although the Five Safes governance framework that applies to National School Data appears to be quite robust, in practice, in 2019 the ICO discovered that the DfE has not implemented national data protection laws properly, and identified 'clear and immediate risks to the DfE's ability to comply with the requirements of data protection legislation', which were an urgent priority to resolve (Information Commissioner's Office, 2020d, p. 2). Defenddigitalme found that the DfE has granted a considerable number of requests for exemptions to the SRS, thereby granting data processors direct access to children's sensitive data, bypassing the Five Safes model, and without due consideration to the rights of the children concerned (Persson, 2020).

In 2011, the then Prime Minister (David Cameron) announced that access to the anonymised NPD data would be opened up to better enable parents, caregivers, and pupils to monitor the performance of their schools in depth. However, defenddigitalme found that, in reality, beyond the stated aim of giving greater transparency to parents, caregivers, and children, access was given to commercial users to create a private sector marketplace for children's public administrative data, which was sensitive and identifying (Department for Education, 2018e; Persson, 2020).

By June 2020, there had been 2000 data shares from the NPD containing personal data, each of which may have included millions of individual records shared with a variety of stakeholders (Department for Education, 2017; Persson, 2020). This is a very high volume of children's sensitive education data shared with various stakeholders, including commercial companies, and without any oversight regarding compliance with data protection laws or child rights frameworks. In January 2020, the Sunday Times reported that data intelligence firm GB Group had been granted access by the DfE to the Learning Records Service, allowing them to access names, ages and addresses of young people aged 14 and over in schools and colleges across the UK for commercial purposes (Bryan et al., 2020).

The original Five Safes framework (outlined above) provides a robust procedure for vetting and controlling access to National School Data. However, undermined by the routine granting of exemptions and bypassing of the five safes framework by the DfE, it is now easier for a commercial entity to access children's education data from the DfE than for an accredited researcher.

Recommendation 2: There is need for a review of the procedures for accessing National School Data from the DfE and for stricter adherence to the Five Safes framework as required by the DEA 2017.

Legal issues for processing children's education data to support their learning

Processing of children's education data by Learning EdTech companies does not come under the DEA 2017 like the DfE/ONS database, so the ONS Five Safes framework does not apply. Instead, only the DPA 2018 and the UK GDPR apply, as well as the AADC, depending on the circumstances.

Applying the UK GDPR to education data

Companies providing Learning EdTech have direct access to children's education data via schools. The school as the primary duty bearer must start by carrying out a DPIA before contracting with a Learning EdTech company. They must then define whether the school or the company is the data controller, and then they must choose a legal basis for the data processing.

The terms on which Learning EdTech companies can process children's education data depends partly on whether they are considered a data controller or a data processor under the UK GDPR and partly on the terms of their contract with the school. The kinds of data that EdTech companies and schools can process and what they can do with them are also determined by the legal basis on which they process the children's education data.

In detailing how the UK GDPR should be applied to children's data, the AADC provides that the child's best interests should be a primary consideration when designing and developing online services that are likely to be accessed by a child (Information Commissioner's Office, 2020a, p. 24). According to this standard, the best interests of the child must be balanced against other interests, for example, the rights of others, but it is unlikely that commercial interests will outweigh a child's right to privacy (Information Commissioner's Office, 2020a, pp. 24-26). However, it is still possible for a company to pursue their commercial purposes while taking into account the best interests of the child. Important considerations for Learning EdTech under the AADC are how to protect and support children's psychological and emotional development and their need to develop their views and identity.

There has been some confusion as to whether or not the AADC applies to EdTech and schools.[33] This confusion highlights a need for clear government guidance on how and when the AADC does apply to schools and to Learning EdTech. In cases where the special protections afforded to children's data accorded by the AADC does not apply to schools, there is also a need for guidance on what does apply in its place.

Data Protection Impact Assessment

Article 35 of the UK GDPR requires a DPIA to be carried out before beginning any type of processing that is likely to result in a high risk. The ICO advises that, in practice, this means that if you offer an online service likely to be accessed by children (which is inherently high risk), you must carry out a DPIA (Information Commissioner's Office, 2020a, pp. 27-31; 2021b, pp. 185-192). Both schools and Learning EdTech companies should carry out a DPIA before using EdTech tools in schools. There is no required template to be used, but the ICO provides a template DPIA as an Annex to the AADC (Information Commissioner's Office, 2020a, pp. 107-113). The DPIA should include a

[33] Defenddigital me contacted the ICO asking for clarification. However, the answer the ICO provided was confusing and inconclusive. Defenddigitalme wrote to the ICO for clarification on whether the AADC applies to EdTech. The ICO responded that where a service is only made available through an intermediary such as a school, the ICO does not consider it to be offered directly to a child for the purposes of Article 8 of the GDPR. But the ICO then said that the AADC does apply to EdTech apps likely to be accessed by a child as long as these can be considered economic activity in a general sense, even if they are funded through subscriptions or advertising revenue. Defenddigitalme concluded that the AADC is independent of Article 8 of the UK GDPR and so the AADC does apply to EdTech regardless of whether consent is the legal basis of processing children's education data by the EdTech company (defenddigitalme, 2020a; 2020b)

description of the processing, which is of particular relevance to Learning EdTech because it requires the data controller to describe the nature, scope, context and purposes of the processing. This includes a description of:

- The intended benefits for children;
- The commercial interests (of the company or third parties that have been taken into account;
- Any profiling or automated decision-making involved;
- Any geolocation elements;
- The use of any nudge techniques;
- Any processing of special category data;
- Any processing of inferred data;
- Any relevant industry standards or codes of practice;
- Responsibilities under the applicable national equality legislation;
- Any relevant guidance on the development needs, wellbeing or capacity of children in the relevant age range.

The data controller must also explain in the DPIA why the data processing is necessary and proportionate for the service. This includes details of measures to ensure accuracy, avoid bias and explain the use of Artificial Intelligence (AI) and specific details about technological security measures in place, such as hashing or encryption standards. The DPIA must also identify the lawful basis for personal data processing under the UK GDPR.

Identifying the data controller and the data processor

Where schools contract with a Learning EdTech company, it is crucial that the data controller is clearly identified because this determines the control the entity[34] has over the purposes and means of data processing and the degree to which they are accountable for complying with data protection laws. Both data controllers and data processors are accountable for data processing, but controllers are more so than processors because controllers are the decision-makers regarding the data uses. The school cannot simply decide to become the data controller because this is a legal definition based on an assessment of the control of the data processing. However, the school can ensure that the terms of their contract with the Learning EdTech company determine the degree to which the Learning EdTech company is permitted to make decisions about education data processing.

Data controllers and data processors

The data controller must decide the purpose and means of data processing. The data controller is responsible for the Learning EdTech company's compliance with the requirements set out at Article 5(1) of the UK GDPR and should be able to *demonstrate*

[34] 'Entity' is used here to refer to an organisation or company with its own legal identity.

compliance with these (European Data Protection Board, 2020). These requirements include: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.

The data processor also has legal duties under the UK GDPR as follows:

- To ensure that persons authorised to process the personal data have committed themselves to confidentiality (Article 28);
- To maintain a record of all categories of processing activities (Article 30(2));
- To implement appropriate technical and organisational measures (Article 32);
- To designate a data protection officer under certain conditions (Article 37);
- A duty to notify the controller without undue delay after becoming aware of a personal data breach (Article 33(2));
- The rules on transfers of data to third countries (Chapter V) apply to processors as well as controllers.

It is quite a complex task to determine who the data controller is, requiring a degree of legal analysis and scrutiny of the EdTech contract and a sufficient understanding of the EdTech company's data processing practices that may be difficult for schools to engage in. In addition, who the data controller is may change on a case-by-case basis, so schools would likely need numerous detailed case study examples to help them to work this out, and such examples do not currently seem to be available.

The UK government guidance on 'Data protection for education providers' simply states that all education providers will either be a data controller or data processor, but does not provide any further guidance on how to decide which applies (Department for Education, 2019c). The ICO guidance states that 'an organisation is not by its nature either a controller or a processor', but rather, this is determined by considering the personal data and the processing activity that is taking place, and who is determining the purposes and the manner of that specific processing (Information Commissioner's Office, 2021c). As part of the same generic guidance for all organisations, the ICO offers an anecdotal example specific to education, of a school that contracts with an EdTech company:

> A private company provides software to process the daily pupil attendance records of a state-maintained school. Using the software, the company gives attendance reports to the school. The company's sole purpose in processing the attendance data is to provide this service to the school. The school sets the purpose – to assess attendance. The company has no need to retain the data after it has produced the report. It does not determine the purposes of the processing; it merely provides the processing service. This company is likely to be a processor. (Information Commissioner's Office, 2021c)

Even in the ICO's case study, we note that they do not definitively find the EdTech company to be a data processor but simply state that this is 'likely to be' the case. Further, the data processing carried out by Learning EdTech companies is generally much more extensive than this example of an administrative EdTech tool, which makes this case study an unhelpful way of explaining how this complex and generic guidance applies to other kinds of EdTech.

Since the school is not defined as a data controller in law, it becomes a question of fact as to which entity decides why and how personal data are processed. This determination is made by an assessment of the factual circumstances, regardless of how the entities are defined in their contract (European Data Protection Board, 2020, p. 9). The European Data Protection Board (EDPB) is an independent European body whose purpose is to ensure consistent application of the GDPR and promote cooperation among the EU's data protection authorities. The EDPB guidelines[35] on the concepts of 'controller' and 'processor' in the GDPR provide the following guidance to determine whether a third party is a data controller or a data processor:

- The level of instructions given to the third party processing the information that determines their degree of independence;
- The monitoring by the data controller of the execution of the service; and
- The expertise of the parties. Where the professional expertise of the service provider plays a predominant role, this may result in them being defined as a data controller in their own right (Forbes Solicitors, 2019).

Entities mandated by law to retain or provide certain data are considered processors with respect to the processing 'necessary' to execute that obligation (Forbes Solicitors, 2019). This would apply to administrative data processed by schools, which they are mandated to provide to the DfE. It may also have applied to the use of learning platforms when schools were mandated to provide access to remote learning during COVID-19. However, the use of other kinds of EdTech, such as Learning EdTech with the purpose of teaching and learning, is more of a grey area because this is arguably not 'necessary' to execute the obligation of teaching and learning, as other methods exist to fulfil this legal duty.

Public database of registered data controllers

The DPA 2018 requires every data controller that is processing personal information to register with the ICO and to pay a fee. The ICO maintains a public, searchable database of all companies and organisations that have registered as data controllers (Information Commissioner's Office, n.d.). It is not clear whether the DfE reviews this list to monitor the number and nature of Learning EdTech companies that are data controllers in the UK. The DfE could use this list as a starting point to maintain oversight of the EdTech companies operating in the UK.

Lawyers in private practice we interviewed for this report advised that, in many cases, both the school and the EdTech company would be independent data controllers. They advised that often the school would be the data controller in relation to data processed by the Learning EdTech company for the purposes of the education and learning of the child, with the Learning EdTech company as the data processor in this instance.

However, the same Learning EdTech company would also be an independent data controller where they process data for their own product development or for marketing to children. In the latter case, the data processing terms would need to be defined in the

[35] The EDPB Guidelines are not binding in the UK and are not specific to the EdTech sector but are useful to interpret the UK GDPR where other guidance is lacking.

contract with the school and the Learning EdTech company would likely rely on the lawful basis of 'legitimate interests'.[36]

Choosing a lawful basis for processing children's education data

Before processing children's education data, the data controller – whether the school or the Learning EdTech company – must choose the lawful basis for processing the data.

The data controller must first determine that the data processing is necessary to achieve the stated purpose, otherwise, no lawful basis will justify processing the data. Whether or not the Learning EdTech data processing is necessary depends on whether it serves an educational purpose, and this is not well defined.[37]

Then, the data controller must choose from one of the six lawful bases under Article 6 of the UK GDPR:

1. *Consent:* Consent must be freely given, and it must be possible to withdraw consent at any time (UK GDPR, Article 4(11)). In the case of Learning EdTech consent could only be freely given where an equally good alternative was offered to children, which is unlikely in a school setting. Consent is the least likely legal basis to apply in a school setting, and should only be considered if none of the other bases apply.[38]
2. *Contract:* Where data processing is necessary to perform a contract with an individual. Children are the data subjects and they are not parties to the contract between the EdTech company and the school so contract does not apply in that scenario. However, where Learning EdTech companies offer children optional extra features it is possible that they would enter directly into a contract with the child at that point.[39]
3. *Legal obligation*: Where data processing is necessary to comply with a legal obligation. This applies, for example, to schools that must collect school census information to share with the DfE. However, it does not apply to Learning EdTech companies because they are not mandated by law to process children's data.
4. *Vital interests*: Where data processing is necessary to protect someone's life.
5. *Public task*: Where data processing is necessary to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. This is the most likely legal basis to be used for the processing of children's education data by Learning EdTech.
6. *Legitimate interests*: Where data processing is necessary for the Learning EdTech company's legitimate interests unless there is a good reason to protect the child's personal data, which overrides those legitimate interests. This cannot apply to a public authority such as a school.

---

[36] Defined at p. 45.

[37] See below, 'What does the public task of education include?', at p. 34.

[38] Consent is, however, required by law for processing children's biometric data, which should not be the case for Learning EdTech (Forbes Solicitors, 2019).

[39] See p. 45 of this report.

Annex C to the AADC advises that, in practice, there are likely to be multiple purposes for data processing, in which case the data controller may have more than one basis for processing (Information Commissioner's Office, 2020a, pp. 101-106). Some of these purposes will relate to core processing activities, and different purposes may relate to non-core processing activities.

Core processing activities

Core processing activities (Information Commissioner's Office, 2020a, p. 102) in relation to Learning EdTech tools likely relate to teaching and learning and come under the public task basis as the tool is being used to perform the public function of educating children.

Non-core processing activities

Non-core processing activities (Information Commissioner's Office, 2020a, p. 103) include:

- Processing for optional elements of the service, which may come under the necessary for contract basis where the child has the capacity to enter into a contract with the Learning EdTech company and has specifically activated the optional elements;
- Processing for broader business purposes such as marketing, service improvement or indirect funding models. These are likely to come under legitimate interests basis. For these to apply, the child must be given separate choices to activate each separate element of the service wherever this is functionally possible. Independent elements of a service cannot be bundled together.

The child (or their parent or caregiver as appropriate) should be given as much choice as possible over non-core elements of processing. In addition, under the AADC, the company should include high-privacy default settings, data minimisation practices and have switch options that use geolocation and profiling off by default.

Conclusion on data controllers and lawful basis in relation to Learning EdTech

According to the above analysis, where a school contracts with a Learning EdTech company to use their product for teaching and learning, it is likely that the school is the data controller for the core purpose of education, under the public task lawful basis. This is true even where the Learning EdTech company offers their service for 'free', in which case an agreement would still need to be signed between the school and the company, including Terms and Conditions of data processing. The school would then be the data processor for this core purpose. However, the Learning EdTech company would be an independent data controller for the non-core purposes that relate to optional extra features that the child can opt into, which would come under the contract lawful basis, and its marketing and product development that would come under the legitimate interests lawful basis. However, it should be noted that one of the experts we spoke to disagreed that children could enter into a contract at all in an educational setting, even for optional extra features of a Learning EdTech tool.

The school as data controller for Learning EdTech

Education data processing on the lawful basis of public task

Where the school is the data controller, the school's legal basis for processing personal information using the Learning EdTech would likely be because it is necessary for the performance of a task in the public interest (UK GDPR, Article 6). We explore below what the public task of education might involve.

Special category data

Article 9 of the UK GDPR prohibits the processing of special category data, such as information relating to race, ethnic origin, politics, religion, trade union membership, genetics, biometric identification, health, sex life or sexual orientation. There are exceptions to this general prohibition, usually referred to as 'conditions for processing special category data', the most likely of which to apply to schools are:

- Explicit consent;
- Vital interests;
- Not-for-profit bodies;
- Legal claims or judicial acts;
- Reasons of substantial public interest (with a basis in law);
- Archiving, research and statistics (with a basis in law).

Where Learning EdTech tools are used to support the learning needs of children with disabilities, and such information may be inferred by the company beyond that which is required under the public task, it is likely that explicit consent would be needed from the child or their parent or caregiver (DPA 2018, Schedule 1(6)(16)). The age at which children are deemed capable of giving consent in the UK is generally considered to be around 13, but this depends on the competence of the individual child (the Gillick competence test established in *Gillick v West Norfolk and Wisbech AHA* [1986] AC 112).

What does the public task of education include?

The ICO provides generic guidance on determining the lawful basis for processing, but information specific to the education sector is limited, and little has been updated since the UK GDPR came into force (Information Commissioner's Office, 2021d). All lawful bases require data processing to be necessary. According to the ICO, 'necessary' does not mean that processing must be essential, but it must be 'more than just useful' and more than just standard practice (Information Commissioner's Office, 2021d). It must be a targeted and proportionate way of achieving a specific purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means or by processing less data.

To answer the 'necessity' question, it is important to first know the specific purpose that the Learning EdTech aims to achieve and what data are being processed. It is then necessary to assess:

- Whether this data processing is targeted and proportionate to meet the identified specific purpose (which involves some assessment of how effective it is likely to be); and

- Whether there is a less intrusive means of achieving the same aim – for example, what if the same money was invested in teachers and tangible classroom resources?

The DfE has identified five key areas of opportunity where EdTech can provide a 'step change', and we are focusing here on Learning EdTech, which relates to one of those key areas: 'teaching practices which support access, inclusion, and improved educational outcomes for all' (Department for Education, 2019d, p. 32).[40] The government does not directly endorse any particular Learning EdTech product for schools or provide any framework for assessing the impact of any particular product, and the responsibility for this is left entirely for schools to determine. In some cases, it may be that these decisions are made by MATs for several schools at once, or sometimes local authorities may advise all schools in their area. The lack of prescriptive government guidance in this area may be intentional to empower schools to make their own decisions regarding the choice of Learning EdTech tools that best suit their own context. In the next phase of this study, we will be asking schools whether they welcome this latitude of choice or whether they find it burdensome.

The EdTech Strategy advises schools that the Education Endowment Fund's (EEF)[41] teaching and learning toolkit reports that studies consistently find EdTech is associated with 'moderate learning gains',[42] including an average of four months' additional progress but with considerable variation in impact (Department for Education, 2019d, p. 48; Education Endowment Foundation, 2019). Given the very different kinds of tech tools included within the EdTech strategy, it is unclear from the strategy whether all of those kinds of EdTech are associated with moderate learning gains, or whether the evidence base is better for some than others, or for some specific products more than others.

Schools must decide whether this kind of impact is 'more than just useful' to meet the necessity threshold as defined by the ICO, and whether the processing of children's data can be justified for this kind of improvement. The EEF notes that 'Evidence suggests that technology approaches should be used to supplement other teaching, rather than replace more traditional approaches. It is unlikely that particular technologies bring about changes in learning directly, but some have the potential to enable changes in teaching and learning interactions' (Education Endowment Foundation, 2019, p. 1). It is an interesting question as to whether schools use the EdTech Strategy and if they do, whether they consult the studies cited in the EdTech Strategy, and whether they see this as empowering or burdensome.

As a subcategory of EdTech, Learning EdTech still includes many different kinds of tech tools, which can usefully be broken down into four further subcategories, as follows:

---

[40] The other three areas are: (i) administration processes that reduce the burden of 'non-teaching' tasks; (ii) continuing professional development that supports teachers, lecturers and education leaders so they can develop more flexibly; and (iii) learning throughout life that supports decisions about work or further study and helps those who are not in the formal education system gain new skills.

[41] The EEF is a UK registered charity and part of the Impetus Private Equity Foundation, which has a £125 million founding grant from the DfE.

[42] It is noted that some experts consulted for this report advised that 'moderate' as used by the EEF here is actually a significant improvement.

- 'Organisational platforms', e.g., Google Classroom, Microsoft Teams or any other platform that allows teachers to manage their classes, assign and collect homework, set their timetable etc.;
- 'Teaching and learning tools', such as simple apps providing digital workbooks to students (e.g., digitalised school book);
- 'Personalised tools' that use algorithms for personalised learning, assessment, teaching and learning (e.g., smart apps such as Dreambox, Imagine Learning, etc.);
- 'Prediction tools' that use algorithms to predict grades or other outcomes.

Where Learning EdTech uses algorithms, such as for categories (iii) and (iv) above, the data controller must have regard to Article 22 of the UK GDPR, which requires companies to carry out a DPIA before using children's personal data for the purposes of profiling children or making automated decisions about them (Information Commissioner's Office, 2021f). Pursuant to Article 22, decisions should not be made about children (or anyone) solely on the basis of automated processing of their personal data, where those decisions have a legal or similarly significant effect on them, unless one of three exemptions apply:

- It is necessary for the performance of a contract between the Learning EdTech company and the child, and the company has put in place suitable measures to safeguard the child's rights, freedoms and legitimate interests;
- It is authorised by UK law, which includes suitable measures to safeguard the child's rights, freedoms and legitimate interests;
- It is based on the child's explicit consent, and the company has put in place suitable measures to safeguard the child's rights, freedoms and legitimate interests.

Ethical Framework for AI in Education

In addition to compliance with data protection provisions, the Institute for Ethical AI in Education has developed an Ethical Framework for AI in Education, which sets out guidance for the design, procurement and application of AI on behalf of learners. The Framework requires decision-makers during the procurement process to insist on relevant information to confirm that AI resources were designed ethically (The Institute for Ethical AI in Education, 2021).

In April 2021, the EU Commission adopted a proposal for a regulation on AI systems, which may become the first ever legal framework on AI, and although the UK is no longer part of the EU, EdTech companies wishing to trade in the EU will need to follow this proposal as it develops (Modrall, 2021).

Recommendation 3: The DfE should produce guidance for companies producing Learning EdTech, which would explain how Learning EdTech must fulfil a defined educational purpose that is supported by robust evidence. The DfE should define in detail the meaning of an educational purpose and maintain an independent evidence base to support this.

The DfE should also provide guidance on the use of experimental learning EdTech tools with no proven evidence base in the school context and rules related to the participation of school children in research trials for commercial EdTech products.

Profiling and automated decision-making by Learning EdTech

For compliance reasons, it is likely to be stated in the Terms and Conditions of most Learning EdTech companies that they only process the 'necessary' amount of data to achieve their stated aims, but whether or not this is true is a question of fact. Under current law, the school must ensure that the contract with the Learning EdTech company sets out exactly which data are being processed and how they are being processed. However, for the school to know which data are necessary to ensure the product's functionality and which are not, they may need to bring in an expert computer scientist to advise their data protection officer. In addition, the school will need to make sure they require the provider to keep them updated on how data processing practices may change further to periodic software updates and new versions of the Learning EdTech product, and ensure that this remains compliant with the law.

Learning EdTech tools sometimes use children's data for profiling or automated decision-making. This can be a feature of products used for personalised learning that use data analytics and aim to identify both skills and strengths in individual children and to detect when children are falling behind and could benefit from an early intervention (Kurni & Srinivasa, 2021, p. 6), both of which a teacher may not otherwise pick up on. Some of these products also use data analytics to profile children and/or their parents or caregivers for commercial purposes.

The Council of Europe (CoE) recommends that profiling of children should be prohibited except in exceptional circumstances where it is in the best interests of the child or where there is an overriding public interest. The CoE recommends that children's attainment and achievement should not be routinely profiled for the purposes of measuring school or teacher performance management as this would not fulfil the definition of an overriding public interest (Council of Europe, 2020, p. 19). However, to determine whether the profiling of the child is in their best interests, it would be necessary to carry out a necessity and proportionality test. The effectiveness of the EdTech tool and the degree to which it is better than a less intrusive alternative such as traditional teaching methods would be important factors in deciding whether the profiling is 'necessary'. The CoE (2020) also recommends following the CoE guidelines on Artificial Intelligence and data protection (2019), where algorithms are used to process children's personal data, which is a feature of personalised learning and profiling of children.

The UNCRC General Comment No. 25 cautions that children may be discriminated against 'when automated processes that result in information filtering, profiling or decision-making are based on biased, partial or unfairly obtained data concerning a child' (United Nations Committee on the Rights of the Child, 2021, para. 10). Understanding the data that Learning EdTech tools are trained on is an important part of assessing whether their use is in the child's best interests. But schools may not have access to this information unless the EdTech company provides an unusually high degree of transparency. UNCRC General Comment No. 25 also calls on states to 'prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling' (United Nations Committee on the Rights of the Child, 2021, para. 42).

Data controllers must also comply with the UK GDPR and may be subject to the AADC in relation to Learning EdTech (see above for a discussion of when and if the AADC applies to schools). Recital 71 of the UK GDPR states that solely automated decision-making, including profiling that has legal or similarly significant effects, 'should not concern a child'. The ICO notes that 'although this wording is not reflected in the Articles of the UK GDPR itself, and so cannot be taken to represent an absolute prohibition on this type of processing in relation to children, it does give a clear indication that such processing of children's personal data should not be the norm' (Information Commissioner's Office, 2021e). However, profiling of children has become a norm for use in personalised learning, grading and learning assessments. The AADC provides that non-essential features that rely on profiling should be switched off by default (Information Commissioner's Office, 2020a, pp. 64-71).

Schools would likely require legal advice to determine whether Learning EdTech products used to personalise children's learning or predict their future performance comply with the UK GDPR and the AADC. This would involve an assessment of whether the data processed by the Learning EdTech company was necessary to achieve the learning or assessment aim, whether its use was in the best interests of the child, whether there was any breach of the child's fundamental rights in the process, and whether there was an easy alternative way of achieving the same learning or assessment aim without processing the same kinds of children's education data or using profiling techniques. In addition, if the Learning EdTech also wants to use the data for commercial purposes, a separate assessment must be made (see below, 'When does the lawful basis of "legitimate interests" apply?').

Can Learning EdTech process data on the lawful basis of public task?

As stated earlier, for public task legal basis to apply, the use of the chosen Learning EdTech product must be effective at meeting an educational purpose; and it must be the least intrusive means of achieving the educational aim.

The government has not produced guidance for schools about which specific Learning EdTech products are or are not effective or how to measure this, and which products are more or less intrusive from a child rights or data protection perspective. Thus, schools are left to make decisions concerning the use of Learning EdTech without sufficiently clear guidelines, yet with full legal responsibility for the resulting data processing.

In order to decide whether Learning EdTech is effective, the EdTech strategy points to a range of external resources. The EdTech Strategy signposts schools to undertake DfE funding training delivered by Future Learn (a private company); to review the DfE-funded special edition of *Impact*, the Journal of the Chartered College of Teaching on EdTech, and the evidence base, which contains 63 different articles behind a paywall (Impact, 2019); to review the EEF recommendations on using digital technology to promote remote learning (Education Endowment Foundation, 2019); to attend British Educational Suppliers Association (BESA) and LearnED continuing professional development (CPD) roadshows where companies market their EdTech products to schools; and to 'try before you buy' by borrowing tech tools for a trial period from the

LendED library run by BESA,[43] which works like a TripAdvisor site for EdTech tools, as schools are invited to rate products they have used. However, one of the articles in the recommended *Impact* journal notes that going on recommendations from peers in other schools constitutes anecdotal evidence.

Recommendation 4: Anecdotal evidence is not a good basis for schools to assess which Learning EdTech tools might be right for use in their context because what works in one school or with one group of children may not work in a different school or with different groups of children. We recommend that the LendED library comes up with a different way to rate products based on formal evidence rather than anecdotal opinions.

First, it is difficult to identify an independent body of research evaluating the impact of various kinds of Learning EdTech that schools could use to make this necessity and proportionality assessment. Some of the entities producing research in this area appear to have a financial interest in endorsing the effectiveness of EdTech. And second, schools do not have the necessary evaluation expertise, or resources, to evaluate the available research and products themselves.

Recommendation 5: It is the government's responsibility as the overall duty bearer to develop an independent oversight mechanism to ensure that EdTech tools used in state schools are both independently evaluated to produce credible improvements in teaching and learning and comply with data protection regulations. A good way to do this would be for the government to develop rules for the procurement of Learning EdTech by schools.

Procurement of Learning EdTech by schools

Government guidance on 'buying procedures and procurement law for schools' advises schools to follow their school's procurement rules, which they can get from their school or local authority. The first option listed is to buy from a framework agreement that allows schools to select a supplier from a list (Department for Education, 2019a). Each framework agreement has details of products, services and suppliers available; agreed pricing structure and Terms and Conditions; and guidance on how to buy (Department for Education, 2016, n.d.-a). The Schools Commercial Team within the DfE assesses several frameworks for compliance with procurement regulations, ease of use, suitability and value for money. Feedback from schools is also considered when selecting these frameworks (Department for Education, 2016, n.d.-b) . The Crown Commercial Service provides guidance for schools on buying ICT goods and technology services through one agreement, but this relates only to hardware and broadband and not to Learning EdTech (Crown Commercial Service & ESPO, 2020).

The government has set out some plans for the future of the EdTech sector in its EdTech Strategy, which states that the government will explore how to facilitate a better online marketplace for EdTech, to help schools and other providers connect with a wide range of trusted, quality products. The premise of this online marketplace is to 'ensure that they are able to draw on the opinions and experiences of their peers, achieve value for

[43] LendED is a platform run by BESA and supported by the DfE that allows schools to borrow EdTech products for trial.

money and [get] help to buy products and services quickly and effectively' (Department for Education, 2019d, p. 20). As discussed above, the opinion of peers represents anecdotal evidence, and it would be better to assess such products against an independent body of empirical research.

The government is also trialling an offer of independent and tailored buying advice through Buying Hubs in the South West and the North West of England, which includes testing a service to manage procurement for schools directly. The stated aim of the pilots is to test models for potential national roll-out. It is unclear what the testing would involve and what criteria the government plans to use to decide which products should be rolled out nationally. There is potential for this approach to take significant pressure off schools, and to provide consistency and quality assurance for the use of EdTech across the UK, provided that the products are assessed according to an independent evidence base and according to their compliance with data protection legislation. Ideally a Child Rights Impact Assessment (CRIA) would be carried out (Livingstone et al., 2021)[44] on all EdTech products under this scheme, as well as a DPIA.

In February 2020, the government accredited six EdTech companies whose apps for pre-school children won a competition for accreditation (Department for Education & Williamson, 2020). The criteria used for assessment were that the apps included elements of play, interaction and ranging levels of difficulty, but seemingly no criteria concerning data protection, safety or the commercial exploitation of children's learning (Persson, 2020).[45] Education Secretary Gavin Williamson said, 'this list of expert-approved apps helps them [parents or caregivers] make confident decisions that benefit their child's language and literacy skills' (Department for Education & Williamson, 2020). We recommend that the government ensures that any expert-approved apps also include a DPIA before being recommended to parents, caregivers, or schools.

Government procurement and funding of Learning EdTech since COVID-19

Against this backdrop of a global gap in governance or oversight of EdTech, the UK government established a £4.6 million innovation fund in partnership with NESTA[46] to try to improve the evidence base for selected EdTech products and oversee their development, but without a focus on data protection. The programme aimed to support the improvement of products and to build an evidence base, but had to be redesigned partway through due to the COVID-19 pandemic. The original programme was designed to support EdTech products to improve their evidence through trialling their products in

[44] For a detailed analysis of CRIA and its use as a tool to realise child rights in the digital environment (Livingstone et al., 2021).

[45] Defenddigitalme found that one of the winning apps, Kaligo (HundrED, n.d.; Persson, 2020b) stored its data on a French server. Its privacy policy did not contain any information about what data are used in its AI algorithms, nor about data used for product development. The app is described as being 'Powered by Artificial Intelligence (AI) and machine learning, the application dynamically defines the learning path to the individual user. If an exercise is not understood, the app will propose new learning exercises until mastered. This customised learning path is also inclusive by design in that people of any age, level and skill can use it. The application also has an enhanced tracking and analysis of each exercise for each user built-in. Currently, no other existing ICT solution has developed an AI engine of this kind.'

[46] NESTA is a UK charity created from a national endowment in 1998 and has since become an independent innovation foundation. (Baker et al., 2019; NESTA, 2016)

schools and colleges in England. The main benefits for EdTech companies would have been improved evidence of the impact of their products through participation in an experimental evaluation carried out with an independent evaluator and a cluster of schools/colleges to live test their products on children. Due to the COVID-19 pandemic, the Innovation Fund was finished early, and the EdTech R&D Programme was established instead to support schools and remote learning EdTech providers.

As part of the EdTech R&D Programme, participating schools and EdTech providers received financial support to cover staff and development costs, specialist evaluation support and professional development. EdTech providers received funding to make developments to their products and implementation processes. The funding focus areas were derived from EEF research and so aimed to be evidence-based. The research suggested that EdTech tools could benefit disadvantaged students in a remote learning context. The project used an independent non-profit evaluator – ImpactED. There is no mention on the website of consideration of data protection compliance.

Recommendation 6: The government has invested significant amounts of money in the Learning EdTech sector without paying sufficient attention to companies' compliance with data protection laws. As a matter of good governance, the DfE should work with the ICO to ensure that these companies comply with the law.

COVID-19 and government contracts with Google and Microsoft

In response to the sudden nationwide transfer to remote learning as a result of COVID-19, the government entered into contracts with Google and Microsoft to provide learning platforms for schools at no cost to them (Flinders, 2020), and with Capita to provide technical support to schools to get set up on each platform (Capita, 2020). The government also established a fund of £14.2 million for schools to cover the technical set-up of the platforms (Trendall, 2021). Schools Minister Nick Gibb said that 'the Microsoft and Google platforms were chosen as they are free to use to the education sector and had the unified technology and support to set up and deliver effective remote education provision, and Google and Microsoft also offer several features and functionalities that are suitable for school needs' (Trendall, 2021). It is unknown whether any assurances were given directly to schools regarding the compliance of Google and Microsoft with data protection laws or on how the AADC applies in this context, and we could not find any government statement on this available in the public domain.

The government's *Keeping children safe in education* statutory guidance[47] (Department for Education, 2020a) signposts schools to obtain remote education advice from The Key for School Leaders (2021a), which is a private consulting company for schools. The Key provides assurances that both Google and Microsoft comply with GDPR privacy and security requirements and have been audited by independent organisations to make sure they meet industry standards (The Key for School Leaders, 2021b). Schools are,

[47] Statutory guidance for education sets out what schools or EdTech companies must do to comply with the law. It should be followed unless there is a very good reason not to. Some guidance must be followed without exception, in which case this is explicitly stated in the guidance document itself. Statutory guidance is different to general guidance, which is generally not binding.

however, advised by The Key that they will still need to check any third party apps (meaning apps that Google or Microsoft does not provide) that they want to use alongside these platforms to ensure they are GDPR-compliant (The Key for School Leaders, 2021b). We cannot say whether The Key provides similar assurances regarding other EdTech companies' compliance with the GDPR because most of their content is behind a paywall. The government does not endorse The Key's advice and takes no responsibility for ensuring that EdTech being used in state schools complies with data protection legislation.

Recommendation 7:

- The Schools Commercial Team, which oversees procurement within the DfE, should develop specific procurement rules for schools entering into contracts with Learning EdTech companies. These should also cover products offered for 'free'. Value for money should be only one criterion for assessment and should not take precedence over children's rights.
- Inclusion of companies on an approved list for schools' procurement should require full compliance with all applicable laws, including the DPA 2018, UK GDPR, HRA 1998, EA 2010 and AADC. Products not on the list should not be procured by schools, even where products are offered for 'free'. This list should replace the current LendED library.
- Compliance must be evidenced by completion of a DPIA and a CRIA. The DPIA should include all the kinds of data the Learning EdTech company intends to process, including personal information, information the company considers to be anonymous, any linked data sets and a detailed explanation of the process used to anonymise any data sets.[1] The DPIA should also include proof of compliance with recognised international cybersecurity standards such as the ISO/IEC privacy and security standards. Learning EdTech that use algorithms should evidence compliance with standards related to the use of AI, such as the Ethical Framework for AI in Education (Institute for Ethical AI in Education, 2021).

Oversight of Learning EdTech compliance with data protection laws

Oversight is a critical governance function performed by an external body to ensure that the law is being properly implemented. In relation to education data protection, oversight of schools and Learning EdTech companies is the responsibility of the ICO that enforces and promotes compliance with the UK GDPR, the DPA 2018 and other data protection legislation. Section 146 of the DPA 2018 provides the ICO with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits. Schools can make a request to the ICO for an audit (Information Commissioner's Office, 2021a), but this is not automatically agreed to, and the ICO lacks the capacity to do this for every school systematically.

An audit by the ICO will typically assess the organisation's procedures, systems, records and activities to:

- Ensure that appropriate policies and procedures are in place;
- Verify that those policies and procedures are being followed;

- Test the adequacy of controls in place;
- Detect breaches or potential breaches of compliance; and
- Recommend any required changes in control, policy and procedure (Information Commissioner's Office, 2021a).

The ICO has the power to conduct compulsory audits under Article 58(1)(b) of the UK GDPR, but it does not so far appear to have carried out a compulsory audit on a school or an EdTech company. There are thousands of State schools in the UK, with 3456 in England alone (Department for Education, 2020b), and it is unlikely that the ICO has the capacity to audit a large percentage of these.

The ICO carried out a consensual audit of 11 MATs between 2018 and 2019 and found that 54% of contracts with data processors did not include compulsory details and terms outlined under Article 28 of the GDPR or security measures the data processor would adopt under Article 32 of the GDPR. Further, 72% did not have suitable procedures in place to ensure processors were meeting GDPR obligations in relation to data breaches, individual rights (Information Commissioner's Office, 2021d) and DPIAs. It also found that the MATs did not complete sufficient periodic checks or audits on processors to provide assurances that they remained in compliance with the GDPR (Information Commissioner's Office, 2019).

A recent ICO compulsory audit of the DfE itself concluded that 'there is no formal proactive oversight of any function of information governance, including data protection, records management, risk management, data sharing and information security within the DfE which along with a lack of formal documentation means the DfE cannot demonstrate accountability to the GDPR.' (Information Commissioner's Office, 2020d, p. 2). The results of these audits are concerning. The fact that 11 MATs demonstrated such a low level of compliance with data protection laws suggests that there is a need to audit all schools systematically and to repeat such audits periodically until schools are in complete compliance with the law. Further, the lack of compliance with data protection laws by the DfE itself suggests that the DfE needs assistance, perhaps from the ICO, in ensuring that the whole education sector understands and implements the laws related to education data governance.

The Office for Standards in Education, Children's Services and Skills (Ofsted) has oversight of schools and carries out inspections related to teaching and learning. Ofsted reports directly to Parliament and is independent of government. Part of Ofsted's mandate is to publish reports of its findings so they can be used to improve the overall quality of education and to inform policymakers about the effectiveness of schools. One of its stated priorities is to ensure that all of its work is evidence-led. However, Ofsted does not currently appear to play any role in assessing the use of Learning EdTech or ensuring it is evidence-based. Although it is not currently part of their mandate, could it be useful for Ofsted to carry out joint inspections of schools with the ICO, so that where Learning EdTech is being used in schools, Ofsted could assess its education utility and the ICO could assess its compliance with data protection laws?

The Office of Qualifications and Examinations Regulation (Ofqual) is a non-ministerial government department independent of government and reports directly to Parliament. Ofqual is responsible for the regulation of national assessments. The chair of Ofqual also chairs the UK Centre for Data Ethics and Innovation (Wakefield, 2020). Ofqual

operates under a Memorandum of Understanding with the DfE, which sets out their commitments to work together, meet regularly, and share information where appropriate (Department for Education & Ofqual, 2018). Ofqual does not currently appear to play any role in assessing the use of Learning EdTech used for assessments and grade predictions outside of national examinations. Although this may fall outside of their current mandate, would it be valuable if Ofqual applied their expertise in the use of algorithms for assessments to assessing the appropriateness of Learning EdTech tools used for assessments and predicting grades?

The Learning EdTech company as independent data controller

As explained above, the Learning EdTech company is likely to be an independent data controller in relation to children's education data processed for non-core purposes, such as optional extra features that the child can opt into. Non-core purposes also include processing education data for commercial or product development purposes. The Learning EdTech company would need to choose the lawful basis of contract for this purpose. It is also likely to be considered an independent data controller when using children's data for its own marketing and product development and would need to choose the lawful basis of legitimate interests for this purpose.

When does the lawful basis of 'contract' apply?

The ICO advises caution in using contract as the lawful basis for processing children's data because this is a complex area of law (Information Commissioner's Office, 2021e). Children are competent to enter into a contract at the age of 16 in Scotland, but in the other UK nations, they are generally considered competent to enter into a contract at age seven, although this is voidable at any time if the child decides. The ICO advises that entities (here, EdTech companies) wishing to process data on the basis of contract should seek legal advice first. Further research will be required to know whether Learning EdTech companies offer extra opt-in features to children and consequently process their data on the lawful basis of contract.

Recommendation 8: As a matter of public policy, the government must set limitations on the contractual terms Learning EdTech companies use to contract with children via schools. The ICO should set out standard contractual clauses for use by learning EdTech companies in relation to data processing. The DfE should set out standard commercial clauses related to price. Any company wishing to deviate from these standard terms should be required to obtain prior permission from the schools Commercial Team within the DfE.

When does the lawful basis of 'legitimate interests' apply to Learning EdTech?

Lawyers in private practice advised us that Learning EdTech companies are likely to process children's data under the legitimate interests basis in practice. This poses problems because, in the absence of Learning EdTech procurement rules, and in a system with little oversight, 'legitimate interests' is the preferred basis for commercial companies and offers the least protections for children.

The ICO advises that legitimate interests is the most flexible of the lawful bases as it is not focused on a particular purpose and therefore gives the data controller more scope to rely on it in many different circumstances (Information Commissioner's Office, 2021g). State schools, including academy trusts, cannot use legitimate interests as their lawful basis for the purposes of delivering education because they are a public authority, and education is a public task[48]. However, learning EdTech companies can use legitimate interests as a lawful basis where they are an independent data controller.

It may be the most appropriate basis when:

- The processing is not required by law but is of a clear benefit to the Learning EdTech company or others;
- There's a limited privacy impact on the individual;
- The individual should reasonably expect the company to use their data in that way; and
- The Learning EdTech company cannot, or does not want to, give the individual full upfront control (i.e., consent) or bother them with disruptive consent requests when they are unlikely to object to the processing (Information Commissioner's Office, 2021g).

The Learning EdTech company must also carry out a legitimate interests assessment that details the nature of the processing and the potential risks it poses to children, and the measures to safeguard against those risks. The company must:

- Identify the legitimate interest;
- Show that the processing is necessary to achieve it; and
- Balance this against the child's best interests, rights and freedoms.

The company is not obliged to publish this assessment or to share it with the school, so this assessment is not likely to be seen or assessed for compliance unless the EdTech company is subjected to a compulsory audit by the ICO (of which there currently is no known case), or unless someone takes the company to court and requires them to produce this assessment as evidence. We recommend that Learning EdTech companies should be required to publish their legitimate interests assessments when using this legal basis as part of our recommended EdTech procurement rules for schools.

The ICO advises that learning EdTech companies must consider what the child might reasonably expect them to do with their personal data in the context of their relationship with the company (Information Commissioner's Office, 2021e). The ICO does not give any specific advice to EdTech companies in this regard. So which data uses a child would reasonably expect is left entirely to the interpretation of the EdTech company, which has a commercial interest in assuming that its data uses are reasonable.

[48] The ICO advises that '…if you are a public authority you cannot use legitimate interests as your lawful basis if the processing is in the performance of your tasks as a public authority. The UK GDPR explains the reason for this exclusion is because it is for the legislature to give public authorities the legal authority to process personal data; i.e., if you are a public authority you should only be able to process personal data in performance of your tasks if the law has given you authorisation' (Information Commissioner's Office, 2021g).

Recitals to the UK GDPR give some examples of the kinds of data processing that would fall under legitimate interests (Bird & Bird, 2020), including Recital 47, which allows for processing for direct marketing or for purposes of preventing fraud.

Article 40 of the UK GDPR encourages supervisory authorities to create codes of conduct in relation to a range of subjects, including the legitimate interests pursued by controllers in specific contexts, as well as the information provided to, and the protection of, children (Articles 40(2)(b) and 40(2)(g)). Such a code of conduct should also contain mechanisms that enable the supervisory authority to carry out mandatory monitoring of compliance with its provisions by the controllers and processors (Article 40(4)).

Recommendation 9: There is a need for the ICO to develop standard contractual clauses for contracts between schools and Learning EdTech companies, detailing the kinds of data that can be processed from children under legitimate interests lawful basis. Despite direct marketing/advertising ordinarily falling under legal basis of legitimate interests, we recommend that as a matter of public policy, and as suggested by CoE Convention 108, Guidelines for data protection in an education setting, Learning EdTech companies are not permitted to engage in direct marketing to children in schools (Council of Europe, 2020). A prohibition on direct marketing to children by EdTech companies could be included in the code of conduct envisaged by Article 40 UK GDPR (see above).

The UK as a global EdTech marketplace

In 2019, the UK government projected that the UK education technology (EdTech) sector would be worth £3.4 billion by 2021, with the largest EdTech export market in Europe (Department for Education, 2019d, p. 27). The leading competitors are identified as being the US, Australia and Scandinavian countries (Department for Education, 2019d, p. 29). Another leading global player in the EdTech market is China (Varghese, 2021).

Evidence indicates that the EdTech industry is a global market driven by a combination of NGOs, commercial enterprises, venture capitalists and philanthropists (Williamson & Hogan, 2020). Key features of this EdTech market are that there is a huge number of products and services on offer to schools, teachers and parents or caregivers, and many of these are offered 'free, for a limited time' (Williamson & Hogan, 2020). Experts interviewed for this report have told us that EdTech companies from other countries contact schools directly and offer free trials of their products. Any governance framework in the UK must cover both standards for UK EdTech companies providing their products in the UK and those seeking to export their products abroad, which makes GDPR compliance an indicator of trust. It must also ensure that EdTech products from outside the UK used in UK schools meet the requirements contained in the UK GDPR and standards in the AADC, including concerning transfer and storage of data outside of the UK.

In the urgency to continue providing education to children worldwide during COVID-19 lockdowns, very little attention has been given to the data protection implications of the EdTech tools deployed globally. The focus has been on access rather than on compliance. Some UN agencies, such as UNESCO (2021) and UNHCR (n.d.), have published lists of EdTech products that enable remote learning during the COVID-19 pandemic. However, UNESCO (2021) notes that these 'do not carry UNESCO's explicit

endorsement' although 'they tend to have a wide reach, a strong user-base and evidence of impact'. No assessment is made of their compliance with data protection laws and standards or their educational value. The UNESCO list includes WeChat Work and YouTube. The UNHCR list includes 645 products on a Google spreadsheet with a description column and a costing column (most of them are free), but nothing related to data protection. The UK government could play a leadership role in this global market by pioneering data protection standards for EdTech, giving UK EdTech products a market edge when some kind of assurance is given about compliance with data protection laws (for example, the GDPR and the California Consumer Privacy Act of 2018 (CCPA)).

Recently more international attention has been paid to data governance for children in general, including education data governance. In 2021 UNICEF published *The case for better governance of children's data: A manifesto* (Day et al., 2021), which calls for all international data governance initiatives to specifically incorporate children's rights into laws and policies. The Manifesto also specifically refers to education data and calls on governments to develop detailed guidelines for schools on the parameters in relation to data processing from children for education purposes and to oversee their implementation (Day et al., 2021). In 2020, the CoE adopted Guidelines on Children's Data Protection in an Education Setting, which were published by the Consultative Committee on EU Convention 108 (Council of Europe, 2020).

Recommendation 10: If the UK wants to lead in the global education marketplace, compliance with the best international standards on data protection and child rights makes good business sense.

Part 3: The way forward

The governance framework that applies to Learning EdTech used in UK schools is complicated, and there is a lack of government guidance for both Learning EdTech companies and schools to follow to ensure they are complying with the law. Currently, a large burden is placed on schools to interpret the law, to choose which Learning EdTech tools are the best for their school, and to work out their own contractual terms with Learning EdTech companies. It is highly inefficient, and possibly ineffective, for each school to duplicate this process. Given the lack of data governance or data analytics expertise in schools, putting the responsibility on schools to negotiate these contracts puts a large amount of power in the hands of EdTech companies to interpret and apply data protection laws in a way that suits their own commercial purposes, without any oversight.

To address these regulatory and implementation gaps, as well as facilitating data sharing in the public interest, this report proposes a staged approach in developing and implementing rights-respecting data governance and oversight of the Learning EdTech sector. The 10 recommendations featured in boxes throughout this report are concrete recommendations which could be implemented immediately. These are based around the need for statutory guidance in relation to education data, from both the ICO with regard to data protection matters and from the DfE with regard to the meaning of 'necessary' use of Learning EdTech for educational purposes. In addition, there should be immediate limitations put on the granting of exemptions to the use of the Five Safes framework for protecting National School Data. Also crucial is the immediate drafting of procurement rules for schools that wish to contract with Learning EdTech companies.

In the medium term there are a number of options that are worth exploring but which require further consideration and research. In the absence of any meaningful government oversight over the tech sector globally or nationally in the UK, it is difficult to define an oversight regime specifically for the Learning EdTech sector. However, below are some suggested steps that could be taken in the medium term to provide more oversight than currently exists, but the final shape this should take is part of an ongoing discussion:

- Experts from Ofsted, Ofqual and the ICO could work together to carry out joint assessments of the educational utility of Learning EdTech in schools, the effectiveness of any assessment or grade prediction tools and their compliance with data protection. This is in addition to the recommendation that the government should vet any Learning EdTech tools before procurement by schools, even where they are offered for 'free'.
- To allow for public and civil society oversight, Learning EdTech companies used in schools could be required to publicly publish their CRIAs and DPIAs prior to being authorised for use in schools.
- The DfE could work with the ICO to maintain a public record of the Learning EdTech companies registered as data controllers via the ICO database.
- The ICO could carry out frequent and random independent audits of Learning EdTech companies on the procurement list. These should be sufficient to encourage

individual EdTech companies to improve company compliance in anticipation of being audited.

- The ICO could develop (initially) a voluntary code of practice for EdTech with a regulatory backstop and penalties for violation, similar to the way in which the Open Internet Code of Practice (Broadband Stakeholder Group, 2016) was developed.[49]

Finally, experts consulted for this report agreed that Learning EdTech companies could be required to share data for use in the public interest. However, some experts were cautious about overemphasising the benefits to children of sharing their education data, and called for the nature of the 'public interest' first to be explained and then strictly adhered to. Again, these ideas require further research and careful consideration, but some suggestions are as follows:

- There could be a requirement that Learning EdTech companies must share data with the DfE and ONS, to be included in the NPD and accessed by accredited researchers.
- EdTech companies could be required to share their data with government-managed data trusts for use in the public interest. The data would need to be de-identified, with strict safeguards to make sure that individuals or groups of children could not be re-identified from any data sets made available to the public. There has been a call for the creation of data trusts from the EdTech sector itself, but it is important that any such initiative is government-led and not defined by the private sector (EdtechUK, 2020).
- The government could explore open standards for learning environments from other jurisdictions, which would enable the sharing of information regarding Learning EdTech tools and their comparison. The Finnish EduCloud is an alliance for the implementation of an open educational cloud service standard (EduCloud), initiated by the Finnish Ministry of Education and Culture (EduCloud Alliance, 2021). EduCloud allows digital learning materials to be produced, acquired and deployed on online learning platforms or other learning network services.
- Options such as those recommended by NESTA could be explored to set up a body in the UK similar to the US Data Quality Campaign (DQC), which has three main aims: to increase public understanding of the value of data in education; to ensure public access to information about data in education; and to improve teachers' and

[49] The Open Internet Code of Practice emerged in response to the issue about Internet Service Providers' management principles of the Internet traffic, or the Net Neutrality debate. The Code is a self-regulatory initiative led by the Broadband Stakeholder Group and supported by the Department for Digital, Culture, Media and Sport, first adopted in 2012 (Department for Digital, Culture, Media and Sport, 2012). The code signalled the UK's preference for a staged approach to regulation, starting initially with self-regulation of ISPs traffic management practices and safeguards against anti-competitive discrimination. In line with this approach, the Office of Communications (Ofcom) stated that it would continue to monitor the effectiveness of this self-regulatory approach and formally intervene if the ISPs failed to comply with the transparency principle set out in the Code or if transparency proved insufficient to deliver the 'best-efforts' internet (Office of Communications, 2011). The UK stood by this approach in the development of the EU regulation on open internet access (Regulation (EU) 2015/2120) – the EU response to the Net Neutrality debate. The Regulation (EU) 2015/2120) lays down the rules to safeguard non-discriminatory internet access services, charging the national regulatory authority, in this case Ofcom, with the duty to monitor compliance and to impose penalties for infringement. The Open Internet Code of Practice has since been updated in line with the requirements of the Regulation (EU) 2015/2120 and with regulatory support from the Regulation (EU) 2015/2120 (Broadband Stakeholder Group, 2016).

leaders' capacity to use data. It brings together different stakeholders to build a consensus, share resources and advocate for changes in policy and practice.

- Lessons could be drawn from the European Commission High-Level Expert Group on Business-to-Government Data Sharing (2020) and its work towards a European strategy on business-to-government data sharing for the public interest. These might include creating a recognised data steward function in both the public and private sectors, awareness-raising for the general public about the societal benefits of data sharing as well as training for public sector staff, and the development of ethical guidelines on data use in the public interest.

The DFC will be looking into these ideas and more as part of its ongoing work on education data governance between now and 2022. It is clear that there is growing international interest in education data governance and in the growing global EdTech sector. The DFC is keen to collaborate with others working on education data governance to identify a comprehensive solution to an urgent child rights challenge of our time.

References

Baker, T., Tricarico, L., & Bielli, S. (2019). *Making the most of technology in education - Lessons from school systems around the world*. https://media.nesta.org.uk/documents/Making_the_Most_of_Technology_in_Education_03-07-19.pdf

Bird & Bird. (2020). *Legitimate interests*. IAPP. https://iapp.org/media/pdf/resource_center/B&B-GDPR-legitimate-interests.pdf

British Educational Suppliers Association. (2017). *BESA Code of Practice*. https://www.besa.org.uk/wp-content/uploads/2017/09/7071-BESA_Code_of_Practice_A4_Download.pdf

British Educational Suppliers Association. (n.d.). *About LendED*. https://www.lended.org.uk/about/

Broadband Stakeholder Group. (2016). *Open Internet Code of Practice 2016*. Retrieved 9 May 2021 from http://www.broadbanduk.org/policies/the-open-internet/open-internet-code-of-practice-2016/

Bryan, K., Griffiths, S., & Ungoed-Thomas, J. (2020, 19 January). Revealed: betting firms use schools data on 28m children. *The Sunday Times,*. https://www.thetimes.co.uk/article/revealed-betting-firms-use-schools-data-on-28m-children-dn37nwgd5

Capita. (2020, 7 May 2020). Microsoft and Google partner with Capita to deliver DfE programme during the Covid-19 crisis. https://www.capita.com/news/microsoft-and-google-partner-capita

Coughlan, S. (2020, 12 August). Students warn mock grades 'make mockery' of exams. *BBC News*. https://www.bbc.com/news/education-53746140

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series - No. 108), (1981). https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

Guidelines on Artificial Intelligence and Data Protection (T-PD(2019)01), (2019). https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

Council of Europe. (2020). *Children's Data Protection in an Education setting - Guidelines*. https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b

Counter-Terrorism and Security Act, (2015). https://www.legislation.gov.uk/ukpga/2015/6/contents/enacted

Crown Commercial Service, & ESPO. (2020). *Education Technology Customer Guidance (RM6103)*. https://assets.crowncommercial.gov.uk/wp-content/uploads/6018-19-Education-Technology-RM6103-GN-June20.pdf

Data Protection Act, (2018). https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Data Protection in Schools. (n.d.). *Sensitive Personal Data – Students*. http://www.dataprotectionschools.com/en/Data-Protection-Guidelines/Sensitive-Personal-Data/Sensitive-Personal-Data-Students/

Data Quality Campaign. (2021). *Home Page*. https://dataqualitycampaign.org/

Day, E., Byrne, J., & Raftree, L. (2021). *The Case for Better Governance of Children's Data: A Manifesto*. https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto

defenddigitalme. (2018). Schools must no longer request pupil nationality data. https://defenddigitalme.org/2018/06/schools-must-no-longer-request-pupil-nationality-data/

defenddigitalme. (2020a). Age Appropriate Design Code applies to edTech. https://defenddigitalme.org/2020/10/age-appropriate-design-code-applies-to-edtech/

defenddigitalme. (2020b). The ICO Age Appropriate Design Code and Schools. https://defenddigitalme.org/2020/09/the-ico-age-appropriate-design-code-and-schools/

Department for Digital, Culture Media & Sport, & Vaizey, E. (2012). *ISPs launch open internet code of practice*. https://www.gov.uk/government/news/isps-launch-open-internet-code-of-practice

Department for Digital Culture Media & Sport. (2020). Explanatory memorandum to the Age Appropriate Design Code. Retrieved from https://www.gov.uk/government/publications/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020

Department for Education. (2016). *Buying for schools (Updated 11 June 2021)*. Retrieved 15 June 2021 from https://www.gov.uk/guidance/buying-for-schools

Department for Education. (2017). Transparency data - DfE external data shares (Last updated 10 June 2021). Retrieved from https://www.gov.uk/government/publications/dfe-external-data-shares

Department for Education. (2018a). *Data protection: a toolkit for schools* (DFE-00119-2018). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf

Department for Education. (2018b). Guidance - How to access Department for Education data extracts. Retrieved from https://www.gov.uk/guidance/how-to-access-department-for-education-dfe-data-extracts

Department for Education. (2018c, 25 September 2018). *National pupil database*. Retrieved 14 June 2021 from https://www.gov.uk/government/collections/national-pupil-database

Department for Education. (2018d). Protection of biometric information of children in schools and colleges - Advice for proprietors, governing bodies, head teachers, principals and school and college staff. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf

Department for Education. (2018e). *Pupils: Personal Records - Question for Department for Education (UIN 120141)*. UK Parliament,.

www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-12-18/120141

Department for Education. (2019a). Buying procedures and procurement law for schools (Updated 22 April 2021). www.gov.uk/guidance/buying-procedures-and-procurement-law-for-schools/find-the-right-way-to-buy

Department for Education. (2019b). Data items 2020 to 2021 - Complete the school census (Updated: 17 May 2021). In. https://www.gov.uk/guidance/complete-the-school-census/data-items

Department for Education. (2019c). *Guidance - Data protection for education providers (updated on 31 December 2020)*. https://www.gov.uk/guidance/eu-exit-guide-data-protection-for-education-providers

Department for Education. (2019d). *Realising the potential of technology in education*. https://www.gov.uk/government/publications/realising-the-potential-of-technology-in-education

Department for Education. (2019e). *Unique Pupil Numbers (UPNs) - A Guide for Schools and Local Authorities (version 1.2)*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/807381/UPN_Guide_1.2.pdf

Department for Education. (2019f). *Using technology in education*. https://www.gov.uk/government/collections/using-technology-in-education

Department for Education. (2020a). *Keeping children safe in education (2020) Statutory guidance for schools and colleges (Updated in January 2021)*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/954314/Keeping_children_safe_in_education_2020_-_Update_-_January_2021.pdf

Department for Education. (2020b). *Number of state-funded secondary schools in England*. Retrieved 5 June 2021 from https://lginform.local.gov.uk/reports/lgastandard?mod-area=E92000001&mod-group=AllRegions_England&mod-metric=2199&mod-period=3&mod-type=namedComparisonGroup

Department for Education. (n.d.-a). *Benefits of using a framework*. https://find-dfe-approved-framework.service.gov.uk/

Department for Education. (n.d.-b). *How frameworks are selected*. https://find-dfe-approved-framework.service.gov.uk/selection

Department for Education, & Ofqual. (2018). Memorandum of Understanding between the Department for Education and the Office of Qualifications and Examinations Regulation. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/749790/Memorandum_of_understanding_between_the_DfE_and_Ofqual.pdf

Department for Education, & Williamson, G. (2020). Early years apps approved to help families kick start learning at home (Press release). In: Department for Education, https://web.archive.org/web/20200224134012/https://www.gov.uk/government/news/early-years-apps-approved-to-help-families-kick-start-learning-at-home

Digital Economy Act, (2017). https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted

EdtechUK. (2020). *EdTech Vision 2025: Interim report from the EdTech Advisory Forum*. www.ednfoundation.org/2020/10/09/edtech-vision-2025

The Education (School Performance Information) (England) Regulations 2007. https://www.legislation.gov.uk/uksi/2007/2324/contents/made

Education Act, (1996). https://www.legislation.gov.uk/ukpga/1996/56/contents

Education and Skills Funding Agency. (2018, 17 June 2021). *Accessing your personal learning record*. https://www.gov.uk/guidance/how-to-access-your-personal-learning-record

Education Endowment Foundation. (2019). Digital Technology - Teaching & Learning Toolkit. https://educationendowmentfoundation.org.uk/evidence-summaries/teaching-learning-toolkit/digital-technology

EduCloud Alliance. (2021). *Home Page*. https://educloudalliance.org/?lang=en

European Commission (High-Level Expert Group on Business-to-Government Data Sharing). (2020). *Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest - Final Report*. https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf

European Data Protection Board. (2020). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR - Version 1.0. Adopted on 02 September 2020*. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en

Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law, 10*(1), 11-36. https://doi.org/10.1093/idpl/ipz026

Flinders, K. (2020, 24 April 2020). Coronavirus: UK schools will get tech support from Google and Microsoft. *Computer Weekly*. https://www.computerweekly.com/news/252482142/Coronavirus-UK-schools-get-tech-support-from-Google-and-Microsoft

Forbes Solicitors. (2019). *A Practical Guide to GDPR for Schools*. Law Brief Publishing. http://www.lawbriefpublishing.com/product/gdprforschools/

Gillick v West Norfolk and Wisbech AHA AC 112, (1986). https://www.bailii.org/uk/cases/UKHL/1985/7.html

HegartyMaths. (2020). *Privacy Notice for Schools Using HegartyMaths*. https://hegartymaths.com/files/HegartyMaths_Privacy_Notice_for_Schools_Update_2020.pdf

Human Rights Act, (1998). https://www.legislation.gov.uk/ukpga/1998/42/contents

HundrED. (n.d.). Kaligo - Digital Handwriting Notebook. https://hundred.org/en/innovations/kaligo-digital-handwriting-notebook#d41dae92

Impact. (2019). Special Issue - Education Technology. *Journal of the Chartered College of Teaching*. https://impact.chartered.college/issue/special-issue-january-2019-education-technology/

Information Commissioner's Office. (2012). *Anonymisation: managing data protection risk code of practice*. https://ico.org.uk/media/1061/anonymisation-code.pdf

Information Commissioner's Office. (2018). Applications - Children and the GDPR. Retrieved from https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf

Information Commissioner's Office. (2019). Findings from the ICO's Consensual Audits of 11 Multi Academy Trusts. Retrieved from https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618610/mats-outcome-report-v1_1.pdf

The Age Appropriate Design Code, (2020a). https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

Information Commissioner's Office. (2020b). *Audits and overview reports - Education sector*. https://ico.org.uk/action-weve-taken/audits-and-overview-reports/education-sector/

Information Commissioner's Office. (2020c). Data sharing across the public sector: the Digital Economy Act codes. Retrieved from https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/data-sharing-across-the-public-sector-the-digital-economy-act-codes/

Information Commissioner's Office. (2020d). *Department for Education Executive Summary*. https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf

Information Commissioner's Office. (2020e). Enforcement Notice to Experian Limited. Retrieved from https://ico.org.uk/media/2618467/experian-limited-enforcement-report.pdf

Information Commissioner's Office. (2020f). *Investigation into data protection compliance in the direct marketing data broking sector* [Investigation Report]. https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf

Information Commissioner's Office. (2020g). The Right of Access (Guide to the General Data Protection Regulation (GDPR)). London Retrieved from https://ico.org.uk/media/for-organisations/documents/2619803/right-of-access-1-0-20210520.pdf

Information Commissioner's Office. (2021a). *A Guide to ICO Audits*. https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf

Information Commissioner's Office. (2021b). Guide to the General Data Protection Regulation (GDPR). Retrieved from https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

Information Commissioner's Office. (2021c). *How do you determine whether you are a controller or processor?* Retrieved 5 June 2021 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/how-do-you-determine-whether-you-are-a-controller-or-processor/

Information Commissioner's Office. (2021d). *Lawful basis for processing*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Information Commissioner's Office. (2021e). *What do we need to consider when choosing a basis for processing children's personal data?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-do-we-need-to-consider-when-choosing-a-basis-for-processing-children-s-personal-data/

Information Commissioner's Office. (2021f). *What if we want to profile children or make automated decisions about them?* Retrieved 5 June 2021 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-if-we-want-to-profile-children-or-make-automated-decisions-about-them/

Information Commissioner's Office. (2021g). *When can we rely on legitimate interests?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/

Information Commissioner's Office. (2021h). *When do we need to do a DPIA?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/

Information Commissioner's Office. (n.d.). *Data protection public register*. Retrieved 5 April 2021 from https://ico.org.uk/esdwebpages/search?EC=3&RegistrationNumber=math

Komljenovic, J. (2021, 11 February 2021). The rise of education rentiers: digital platforms, digital data and rents. *Learning, Media and Technology*, 1-13. https://doi.org/10.1080/17439884.2021.1891422

Kurni, M., & Srinivasa, K. (2021). Introduction to Learning Analytics. In *A Beginner's Guide to Learning Analytics* (1 ed., pp. 1-28). Springer. https://doi.org/10.1007/978-3-030-70258-8

Landau, S. (2018, 26 February). Understanding Data Breaches as National Security Threats. https://www.lawfareblog.com/understanding-data-breaches-national-security-threats

Livingstone, S., Mukherjee, S., & Pothong, K. (2021). *Child Rights Impact Assessment - A tool to realise children's rights in the digital environment* [Report]. DFC - 5Rights Foundation. https://digitalfuturescommission.org.uk/wp-content/uploads/2021/04/CRIA-Report-revised-final.pdf

Modrall, J. (2021, April 2021). *EU proposes new Artificial Intelligence Regulation*. Norton Rose Fulbright. https://www.nortonrosefulbright.com/en/knowledge/publications/fdfc4c27/eu-to-propose-new-artificial-intelligence-regulation

National Center for Education Statistics. (2016). *Forum Guide to Education Data Privacy (National Forum on Education Statistics 2016-096)*. https://nces.ed.gov/pubs2016/nfes2016096.pdf

Nesta. (2016). *Making the most of data in schools*. https://media.nesta.org.uk/documents/Making_the_most_of_data_in_schools_-_FINAL.pdf

Office for National Statistics. (2020a). *Accessing secure research data as an accredited researcher*. https://www.ons.gov.uk/aboutus/whatwedo/statistics/requestingstatistics/appr

ovedresearcherscheme#becoming-an-accredited-researcher-under-the-digital-economy-act-2017

Office for National Statistics. (2020b). *Assured Organisational Connectivity to the Secure Research Service (Accessing secure research data as an accredited researcher)*. https://www.ons.gov.uk/aboutus/whatwedo/statistics/requestingstatistics/approvedresearcherscheme#safe-setting-access

Office for National Statistics. (2020c). *The Five Safes (Accessing secure research data as an accredited researcher)*. Retrieved 5 April 2021 from https://www.ons.gov.uk/aboutus/whatwedo/statistics/requestingstatistics/approvedresearcherscheme#the-five-safes

Office of Communications. (2011). Ofcom's approach to net neutrality. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0011/50510/statement.pdf

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA law review, 57*(6), 1701-1777. https://heinonline.org/HOL/P?h=hein.journals/uclalr57&i=1713

Persson, J. (2020). *The State of Data 2020: Mapping a Child's Digital Footprint Across England's State Education Landscape*. https://defenddigitalme.org/state-of-data/#h.aah28dqhbad

The Privacy and Electronic Communications (EC Directive) Regulations, (2003). https://www.legislation.gov.uk/uksi/2003/2426/contents/made

Protection of Freedoms Act, (2012). https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology, 10*(1), 40-81. https://doi.org/10.1080/17579961.2018.1452176

Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retai charges for regulated intra-EU communications and amending Directive 2001/22/EC and Regulation (EU) No 531/2012. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02015R2120-20201221&from=en

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Ridgeway Primary Academy. (n.d.). *Google Classroom Notice to Parents and Guardians*. https://www.ridgewayprimaryacademy.co.uk/google-classroom-notice-to-parents-and-guardians/

Ritchie, F. (2017). The 'Five Safes': a framework for planning, designing and evaluating data access solutions. https://doi.org/10.5281/ZENODO.897821

Show My Homework. (n.d.). *Show My Homework Privacy Policy*. https://www.satchelone.com/smhw-privacy-policy

The Institute for Ethical AI in Education. (2021). *The Ethical Framework for AI in Education*. https://fb77c667c4d6e21c1e06.b-cdn.net/wp-content/uploads/2021/03/The-Institute-for-Ethical-AI-in-Education-The-Ethical-Framework-for-AI-in-Education.pdf

The Key for School Leaders. (2021a). *Authoritative Knowledge for School Leaders Who Are Making a Difference*. https://schoolleaders.thekeysupport.com/

The Key for School Leaders. (2021b, 8 January 2021). Mythbuster: 7 misconceptions about digital education platforms. https://schoolleaders.thekeysupport.com/covid-19/deliver-remote-learning/make-tech-work-you/mythbuster-misconceptions-digital-education-platforms/

Trendall, S. (2021). Schools offered £14m to set up on Google or Microsoft learning platforms. https://www.publictechnology.net/articles/news/schools-offered-£14m-set-google-or-microsoft-learning-platforms

UK General Data Protection Regulation (UK GDPR), (2020). https://www.gov.uk/government/publications/data-protection-law-eu-exit

UK Home Office. (2021). Statutory Guidance - Revised Prevent Duty Guidance: for England and Wales. Retrieved from https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales

UK Statistics Authority. (2019a). Accredited Researcher Application Guidance. Retrieved from https://uksa.statisticsauthority.gov.uk/wp-content/uploads/2019/07/DEA_Accredited_Researcher_Application_Guidance_v1.0.pdf

UK Statistics Authority. (2019b). Research Project Accreditation Application Guidance. Retrieved from https://uksa.statisticsauthority.gov.uk/wp-content/uploads/2019/07/DEA_Research_Project_Application_Guidance_v1.1.pdf

UK Statistics Authority. (2020). Research Code of Practice and Accreditation Criteria (Guidance). Retrieved from https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice/research-code-of-practice-and-accreditation-criteria

UNESCO. (2021). *Distance learning solutions*. https://en.unesco.org/covid19/educationresponse/solutions

UNHCR. (n.d.). Digital Learning Resources List. In. https://docs.google.com/spreadsheets/d/1Yn2rrbhHViGDMPvrioQPmXStWT2gQzH3rIKV60KTaHw/edit#gid=1092357953

General Comment No. 25 on Children's Rights in Relation to the Digital Environment (CRC/C/GC/25), (2021). https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, (1966). https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

Varghese, T. (2021, 13 May 2021). Covid-19 has reinforced China's role as global leader in EdTech. *The Times Higher Education*. https://www.timeshighereducation.com/campus/covid19-has-reinforced-chinas-role-global-leader-edtech

Wakefield, J. (2020, 20 August). A-levels: Ofqual's 'cheating' algorithm under review. *BBCNews*. https://www.bbc.com/news/technology-53836453

Walters, R. (2021, 14 January 2021). UK EdTech sector grows to £3.5bn as demand surges for digital classrooms and AR. https://www.fenews.co.uk/press-releases/61610-uk-edtech-sector-grows-to-3-5bn-as-demand-surges-for-digital-classrooms-and-ar

Williamson, B. (2021, 28 May 2021). Google's plans to bring AI to education make its dominance in classrooms more alarming. *Fast Company*. https://www.fastcompany.com/90641049/google-education-classroom-ai

Williamson, B., & Hogan, A. (2020). *Commercialisation and privatisation in/of education in the context of Covid-19*. Education International,. https://eprints.qut.edu.au/209028/