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

5RIGHTS FOUNDATION

A Blueprint for Education Data

Realising children's best interests in digitised education

Digital Futures Commission

MARCH 2023

Contents

Definitions

Education data is personally identifiable information relating to children processed in or through schools. It includes data collected or inferred by education technology (EdTech) providers of multiple and sometimes overlapping functions including administration and management information systems (MIS), learning and assessment (e.g., Google Classroom, ClassDojo, MyMaths) and safeguarding (e.g., CPOMS [Child Protection Online Management System] and other Safety Tec).

For simplicity, 'school' includes any educational establishment providing primary or secondary education, whether a local authority, academy or private educational institution.[1]

Why do we need a blueprint?

School is compulsory for almost all children. It is central to their childhood and their path to adulthood. If children must be at school, it surely follows that their rights must be upheld in school settings, including their right to data protection.

The introduction of EdTech in schools has not always provided a safe and secure environment.[2] As this blueprint sets out, there is widespread invasion of children's privacy, little evidence to support the claimed learning benefits, and perhaps most important in the long run, no grand plan for using children's data in their best interests.

This is a nascent sector with the potential to make life-changing differences to young people's life chances. To create benefit, however, we must first understand what education data is, who is currently harvesting it, and how we might restructure the somewhat confused regulatory environment. The status quo creates an unacceptable asymmetry in which commercial players get unfettered access to children's education data to the detriment of children's privacy while such data remain largely unavailable to and unused by those who could deliver the insights that might actually benefit children and educators.

The ambition of this blueprint is not to provide a gold standard for all players in the EdTech ecosystem, although we welcome those companies and educators who set themselves that goal. Rather, it sets out the baseline for data processing, which businesses and schools must not fall.

This baseline will be achieved by:

1. Clarifying, and where necessary, extending the relevance of existing frameworks that protect children's data to ensure a coherent regulatory environment.
2. Introducing certification to ensure compliance and measure learning benefits for EdTech used in school settings.
3. Developing trusted data infrastructure(s) for research, business and government that serve the best interests of children and the wider educational community.

[1] Education Act 1996, Section 4.
[2] See Annex 1.

The blueprint's three sections address issues of data governance, argue for certification of EdTech, and look at ways of data sharing in the best interests of children and the broader education community. While the last section is the least detailed, it includes some bold steps towards a new, more ambitious, regime that must surely be the ultimate goal, even as we bring clarity and fairness to bear on existing arrangements.

Basic principles

The blueprint embodies children's existing rights. Children's rights are already codified in the United Nations Convention on the Rights of the Child (UN, 1989), ratified internationally, and applicable in the digital environment, as set out in General Comment No. 25 on children's rights in relation to the digital environment (UN Committee on the Rights of the Child, 2021).

The blueprint realises children's right to education and protection from commercial exploitation.[3] A child should be able to access education free from commercial exploitation of their data.[4] This does not mean that it is not possible to make a commercial return on EdTech products, but rather, that data-driven EdTech must be transparent about the exchange instead of generating excessive economic profits from children's data or the labour of teachers, or offering a foothold for extraneous commercial activity. Instead, EdTech should deliver evidence-based public and educational benefit in the best interests of children.

The blueprint is tech neutral. While some specific companies are referred to in this document, this blueprint should not be understood to apply only to a particular technology or service, and nor does it exempt others. The way education data is collected, processed, used, stored and shared must consider children's rights in the round, irrespective of the technical approach or purported outcome.

The blueprint welcomes a mixed economy of EdTech in which children's best interests are paramount. Both government and commercial organisations play an important role in the provision of EdTech, which is why getting the governance framework right is so vital. Many EdTech products as currently configured do not adequately consider or enforce the 'best interests' of the child in their deployment or governance. The blueprint sets out how we can reset the balance between commercial interests and the best interests of the child.

Roles and responsibilities

Schools and teachers: An important outcome of the blueprint is to address the power imbalance between digital providers and schools, including a school's governing body, teachers, data protection officers (DPOs) and advisors. Establishing agreed standards of privacy, safety, security and educational benefits that are meaningfully enforced through

[3] Articles 28 and 32 of the UNCRC.
[4] Commercial or economic exploitation is defined as 'taking unjust advantage of another for one's own advantage or benefit [and] covers situations of manipulation, misuse, abuse, victimisation, oppression or ill-treatment' for 'material interest' or gain (OHCHR, 1993).

regulation and certification would enable schools to focus on procuring technology that supports their students' educational outcomes and best interests.[5]

Developing trust in EdTech businesses: The EdTech sector must be incentivised and enabled to benefit from protecting and respecting children's best interests. This should encompass compliance with safety, security, privacy and data protection standards, using certification to incentivise compliance with these standards across the EdTech sector. Certification will support schools in navigating the diverse EdTech market.

Government has a key role, particularly the Department for Education (DfE) and Department for Science, Innovation and Technology (and formerly, the Department for Culture, Media and Sport, that has been largely silent on the matter of education data). Until now there has been a failure to tackle the known problems of EdTech, and a reluctance to interrogate the role of commercial players operating in school settings in relation to the quality of their contribution and the impact on children's privacy, learning outcomes and prospects. By innovating in trusted data sharing and embedding quality and standards, the UK will foster a vibrant EdTech sector that contributes meaningfully to children's education.

The world of data is going to change. The move to create data trusts is generating interest, and distributed technologies will require further reimagining of what data equity, effective stewardship and data protection could look like.[6] This is why an independent and effective research mechanism – in the public interest – that also explores policy options is central to the blueprint. The education sector and businesses need policy and regulatory certainty, and this will, in turn, provide clarity and accountability that can benefit all stakeholders in articulating the value and operation of EdTech.

Nothing in this blueprint pre-empts or prevents a better system of data sharing. It anticipates and encourages innovation on the basis that future systems are designed in children's best interests. We urge government, regulators and businesses to grasp the opportunity outlined in this blueprint. Without harmonising the regulatory landscape and creating trust in the EdTech sector and its data ecology, we will miss the opportunity to be at the forefront of research, innovation and children's right to education without commercial exploitation.

The UK government's Data Protection and Digital Information Bill 2022 presents an opportunity to enshrine the blueprint in legislation and to reassert the importance of protections for children provided by the Age Appropriate Design Code (AADC) (ICO, 2020) and the Children Act 1989 and 2004. Many of the actions necessary to address current uncertainty and reallocate responsibility do not require new legislation and could be acted on by relevant bodies as a matter of urgency. While the blueprint is focused on the UK, it provides a framework for what 'good' looks like that could be adapted by other jurisdictions.[7]

[5] See Turner et al (2022).
[6] See Royal Society (2023) and Taylor (2022).
[7] We are grateful to those colleagues outside the UK who have contributed to its development. We have also drawn on the work of key international organisations, including the Broadband Commission, Council of Europe, UNESCO and UNICEF.

Three priorities for education data governance

1. Clarify, and where necessary, extend existing frameworks to protect children's data

1.1. Routinely uphold the United Nations Convention on the Rights of the Child

The United Nations Convention on the Rights of the Child (UNCRC) codifies children's rights for signatory countries, and as a signatory to the Convention, the UK is obliged to consider it in legislation and regulation. General Comment No. 25 (2021) interprets the application of the UNCRC to the digital environment. Widely adopted and well respected as the most comprehensive document concerning children's rights online, it offers guidance to all stakeholders towards realising children's rights in digital settings (see Box 1).[8]

Box 1: The impact of citing the UNCRC

Referencing the UN Convention on the Rights of the child (UN, 1989) in the AADC, a statutory code of practice required under Section 123 of the Data Protection Act (DPA) 2018,[9] has three notable implications.

It recognises that children's rights – including the protections afforded by the AADC – apply to all children under 18, based on the UNCRC definition of a child that transformed the industry norm of considering 13 as the age of adulthood.

The UNCRC establishes that data protection should take children's 'best interests' – as 'a right, a principle and a rule of procedure' (CRC/C/GC/14, p 3) – as a primary consideration. As the Information Commissioner's Office (ICO's) (2022a) Best Interests Framework sets out, this means digital providers should provide for children's diverse requirements for safety, health, wellbeing, familial connections, development, agency and other rights and freedoms. General Comment No. 25 extends the application of best interests beyond data protection to all aspects of the digital environment that impact on children's rights.

Finally, and perhaps most importantly, it enables children to directly rely on the UNCRC when seeking to enforce their rights.

Action 1: The UNCRC and General Comment No. 25 should be explicitly referenced in all existing and future law, policy and practice relating to children's education data.

1.2. Robustly apply the Age Appropriate Design Code

The ICO's AADC is a statutory requirement of the Data Protection Act 2018 and is considered the 'gold standard' in children's data protection, leading the way globally in articulating data protection requirements on Information Society Services (ISS) in relation to

[8] Signatories are required to ensure children benefit from a holistic, rights-respecting approach to the processing of their education data through a range of measures including jurisprudence on children's 'best interests' and evolving capacities, and measures of implementation such as child consultation, child rights due diligence, a child rights impact assessment and child-friendly materials.
[9] Data Protection Act (DPA) 2018.

children. The AADC has led to notable improvements by some of the biggest companies in the world[10], and is being mirrored in other jurisdictions.[11]

However, many EdTech products and services that meet the criteria of ISS fail to comply with the AADC. One reason is that schools fit the definition of intermediaries that use EdTech products and services to perform the 'public task' of education. This allows EdTech providers to evade their responsibilities under the AADC,[12] which undermines the effectiveness of the AADC and fails children in an environment in which they are the main data subjects (see Box 2).

Box 2: Enforcement of the Age Appropriate Design Code

ICO investigation into TikTok[13]

TikTok could face a £27 million fine after an ICO investigation found that the company may have breached UK data protection law, failing to protect children's privacy when using the TikTok platform. The ICO has issued TikTok Inc. and TikTok Information Technologies UK Limited ('TikTok') with a 'notice of intent', a legal document that precedes a potential fine. The notice sets out the ICO's provisional view that TikTok breached UK data protection law between May 2018 and July 2020. The ICO investigation found that the company might have:

- processed the data of children under the age of 13 without appropriate parental consent;
- failed to provide proper information to its users in a concise, transparent and easily understood way; and
- processed special category data, without the legal grounds to do so.

Information Commissioner John Edwards said: "We all want children to be able to learn and experience the digital world, but with proper data privacy protections. Companies providing digital services have a legal duty to put those protections in place, but our provisional view is that TikTok fell short of meeting that requirement."

According to the ICO, as well as 'building relationships' with companies to 'influence their approach to data protection',[14] enforcement of the AADC is required when companies do not respond positively to the regulator's guidance.

The AADC should be robustly applied across all digital products and services that process personal data about children. This includes all uses of EdTech, irrespective of types of use,

[10] 5Rights Foundation (2022).
[11] Stokel-Walker (2021).
[12] EdTech products and services that require children – students – to directly interact with the products or services, including through account creation and log in, meet the criteria of an ISS, and therefore the AADC applies. These requirements involve an 'individual request' for data to be transmitted via 'electronic means' and 'at a distance' (Directive (EU) 2015/1535). Examples of these EdTech products and services currently used in UK schools include Google Classroom, ClassDojo and MyMaths. MIS used in schools, including safeguarding software, on the other hand, do not meet the criteria for ISS because children do not 'individual[ly] request' the service (Directive (EU) 2015/1535). Although the AADC does not apply to them (because they are not ISS), the ICO has stated that the principles codified by the AADC should be adhered to by MIS.
[13] See ICO (2022c).
[14] ICO (2022d, p 2).

and must include 'core' and 'additional' services, 'off the shelf' services and those tailor-made for the school. The AADC should also apply whether the child uses the service directly or has no direct contact with the service, but the school uses it to record data about the child.[15] The same high bar of data protection should also be required of MIS and any other school systems that hold the child's data. The AADC has a 'best interests' exemption that allows business, regulator and schools to override one or more of its standards, which allows for innovation and exceptions that are in best interests of the child.

Action 2: The government should use the Data Protection and Digital Information Bill 2022 to clarify that all EdTech that process data about children must meet the data protection and privacy baseline provided by the AADC.

1.3. Comply with the UK GDPR

A data controller is responsible for the purpose and means of data processing, and is required to comply with the requirements of Article 5 of the UK General Data Protection Regulation (GDPR): lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality. In practice, schools often control data jointly with EdTech providers (see Box 3). This can occur when:

- schools sign contracts that fail to limit the purpose of processing;
- the contract says that the school is the data controller, but the EdTech impedes the school's capacity to exercise control (see Box 3);
- providers process data that schools did not foresee, for example, keystroke dynamics or inferred data;[16]
- providers process data in ways that exceed the schools' purposes (such as for marketing or Research & Development [R&D]).

> *"[Times Tables Rock Stars] say we're just the processor. But then they have this thing where they say we use the data for what we want, including they'll give it to the government or use it for research purposes. And you get this feeling that the schools aren't the one with the power, because they're under pressure to deliver educational provision, particularly in the pandemic."* (Local authority DPO)[17]

[15] Data about children are also recorded in school MIS. There are grounds for believing that MIS does not comply with these principles (e.g., the news story in Box 8.

[16] This is particularly the case where the contract permits the use of a child's data for Research and Development (R&D) purposes, advertising or marketing. This data is not processed for the lawful basis of public task, the school does not control its onward use and in the absence of other lawful basis, the data subject is not always given the opportunity to consent to either the contract or the processing.

[17] See Turner et al (2022).

Box 3: Control of data and purpose limitation

A highly technical Data Protection Impact Assessment (DPIA) of G Suite for Enterprise (the predecessor to Google Workspace for Education), conducted by Privacy Company[18] in the Netherlands, concluded that, because of the interaction between different Google products, the collection of service and telemetry data coupled with the inability of a customer to be aware of the purposes for which data was processed, Google collects and uses customer personal data as a controller or joint controller with the customer.[19] Some of that data may be personal data of a sensitive nature, or it comes within 'special categories' of personal data revealing protected characteristics.[20] In the context of Google used in a school, the school would be the 'customer' with a contract with Google.

Although this categorisation as controller or joint controller was not accepted by Google, following negotiations, Google agreed to limit data processing in their contract with Dutch schools and universities to three specific purposes rather than the multiple general purposes set out in the Google Cloud Privacy Notice.[21] This solved some of the high data protection risks identified in their DPIA where Google and the universities were factually acting as joint controllers (irrespective of what was contained in the DPIA). Google has stated that this requires a technical redesign.

The ICO provides a checklist for organisations to self-assess whether they are data controllers, processors or joint controllers. But this checklist does not work well in an educational context where the controller acts as an intermediary for a child.

At the content level, the checklist fails to account for the contractual relationship between EdTech providers and schools, which is complicated by a school's status as an intermediary mediating between EdTech providers and children as the data subjects (see Box 3), and is insufficiently clear about the requirements of purpose limitation and lawful basis in those circumstances. At the procedural level, the checklist does not require organisations to provide evidence to substantiate their answers to any items in the checklist. This results in EdTech providers describing themselves as processors in contracts despite actually being controllers or joint controllers. At the enforcement level, the checklist is voluntary guidance, and there is no evidence that EdTech companies or schools are using it.

Any checklist that is designed to identify the controller in a true sense needs to:

- recognise and identify the differences between types of data collection in education, including data collected under statutory requirements, interaction data and inferred data;
- identify particular problems arising as a result of schools acting as intermediaries between EdTech providers and children (as users);
- identify whether the use of particular digital technologies in education is necessary and proportionate to the aim sought;

[18] Much of this analysis was conducted by examining audit logs and available telemetry data to determine what data was collected (Nas & Terra, 2021a, 2021b).
[19] This assertion was not accepted by Google DPIA but it has since agreed to limit the purposes (Nas & Terra (2021a, 2021b).
[20] See Nas & Terra (2021a, p 64).
[21] See Nas & Terra (2021b).

- determine whether the school retains the necessary control to be the data controller;
- identify the correct lawful basis for processing children's data, including guidance as to education as a public task;
- restrict the data processor's processing activities to specified purposes;
- ensure consent is informed, freely given and only relied on where necessary.

Action 3: The ICO should develop an education-specific checklist to identify the controller in practice. Where there is a lawful basis for EdTech providers to become joint controllers, it must be possible for each party to fulfil their data controller responsibilities proportionate to the volume, variety and usage of the data they process without overburdening the other. In all cases, responsibilities must not be put on to those who cannot in practice fulfil them.

1.4. Ensure transparency

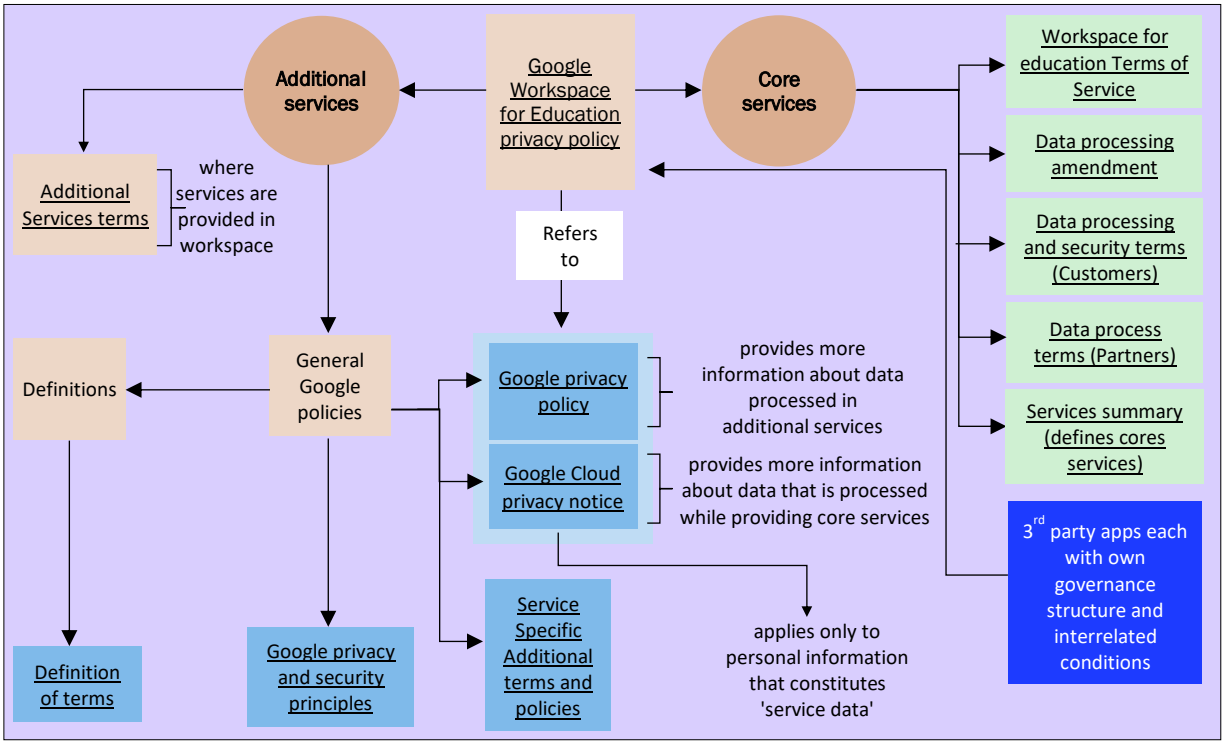
Transparency and high standards of compliance from EdTech providers is required when different data protection and privacy policies apply to different products accessible within a single learner journey. Google Workspace for Education illustrates the problem of lack of transparency and compliance (see Box 4).[22]

Box 4: Google Classroom governance structure

Google Workspace for Education – a hybrid teaching/learning and school management system – offers 'Core Services',[23] including Google Classroom, Docs, Sheets, Drive, Meet and Hangouts. Within this virtual platform, 'Additional Services'[24] such as YouTube, Maps and Search can be enabled by schools, and are therefore visible and available to a child within a single learner journey.

However, these Core and Additional Services are governed by different privacy policies and legal terms that offer different levels of privacy protection to the same child in their online learning journey through the Google Workspace. Crucially, Google does not use data processed from children to create profiles used for targeted advertisements while the child is using Core Services, and nor are children shown advertisements while using Core Services. Such protections do not apply automatically to Additional Services.

[22] Unless the clip hosted by YouTube or Vimeo is embedded in the Google Classroom environment.
[23] 'Core Services' are Google's main applications within the Google Workspace for Education platform.
[24] 'Additional Services' are Google's consumer applications accessible through the Google Workspace for Education platform if the school's platform administrator allows pupils to access them.



Interface design can facilitate children's unintentional use of additional services offered by the provider as well as services operated by other providers that offer weaker privacy protection than Core Services. This can result in a child's data being used in ways that are not transparent to the learner or school. It may make a child's school data available in commercial contexts, leaving them open to commercial exploitation and at risk of future discrimination (see Box 5).

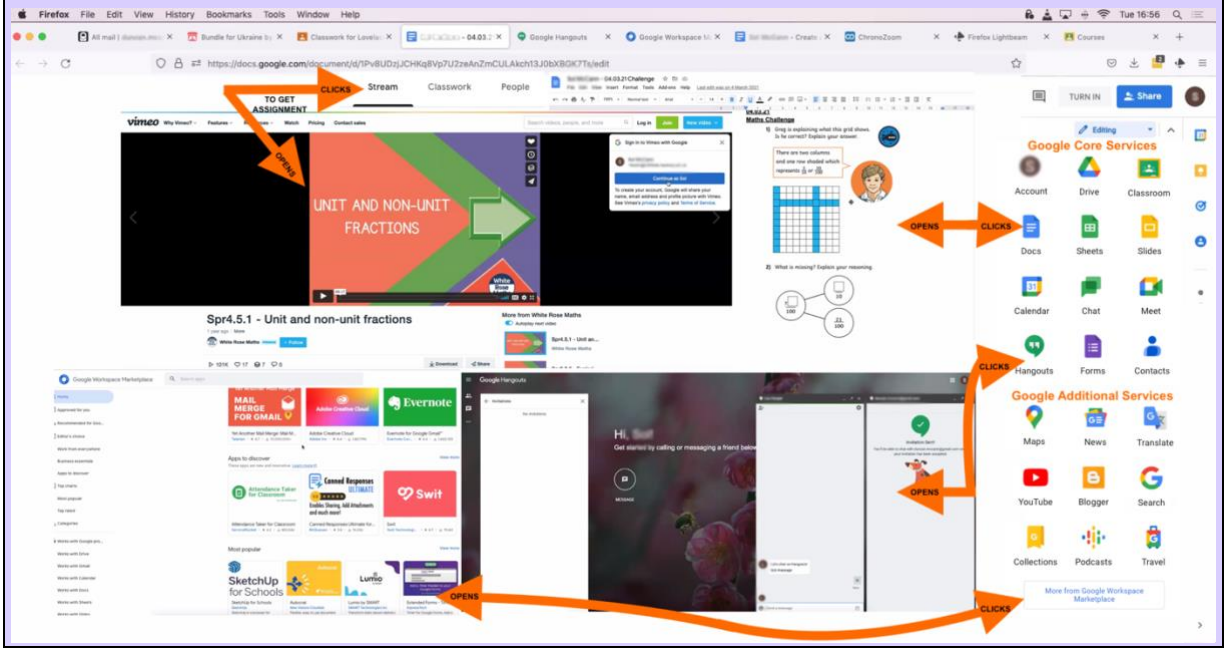
Box 5: Lightbeam's identification of third party tracking via Google Classroom

We conducted an experiment with Google Classroom to see how it was used by a nine-year-old child in a primary school in London and a twelve-year-old child from a different school during COVID-19 lockdowns. Both children were exposed to Google Classroom settings that facilitated access to both 'Core' and 'Additional Services' – the former is privacy-preserving, the latter is not. There was no notification to inform the child user when they moved to a different privacy regime, or any additional request for consent. Since the children were provided access to both Core and Additional Services – even non-Google services – to carry out their schoolwork, it also appeared that Google did not make schools aware of this distinction, or the different privacy policies that apply.

In one instance, when a child clicked on a link using learning material hosted on Vimeo, Lightbeam's data capture[25] showed that the child's access to the learning material hosted on Vimeo was tracked by 42 third parties, including 'adservice.google.co.uk', 'analytics.tiktok.com', 'amazon-adsystems.com' and others. When the child later clicked on YouTube, they were subject to cookie surveillance by a further 50 third party sites.[26]

[25] Lightbeam is an internet browser add-on, offered by Mozilla, that visualises the first and third party tracking cookies companies deploy to monitor users' browsing habits (Fowler, 2013).
[26] Adapted from Hooper et al (2022).

A nine-year-old's user journey through Google Classroom



If a learner's journey involves moving from one EdTech product or service to another, then the highest bar of privacy protection should be applied by the EdTech provider to all the services whose use is required by the school. This is consistent with Action 2 (the ICO is to robustly enforce data protection regulation including the AADC for all EdTech).

Where an EdTech provider processes data from a child for a non-educational purpose, this must be either under an individual contract with the child or a legitimate business interest (which requires that the child is given separate choices to activate each separate element of the service, that is, the elements cannot be bundled).[27]

To address the problem of over 20,637 state-funded English schools[28] having to negotiate individually with EdTech companies, DfE guidance is vital as part of a school's procurement processes. The Dutch Data Protection Authority's negotiation with Google sets an example for how a centralised agreement or guidance to establish a minimum standard of practice[29] could relieve schools from the power imbalance and burden of contract negotiation (see Box 3).

Action 4: The DfE should develop, with the support of the ICO and/or Crown Commercial Service, standard contractual clauses for schools to insert into their contracts with EdTech providers. These should restrict EdTech's data processing to the processing purposes that schools choose and can reasonably audit.

[27] See Day (2021).
[28] BESA (n.d.).
[29] See Nas & Terra (2021b).

2. Introduce certification for EdTech used in school settings

2.1. The need for an approved framework and standard EdTech assessment criteria

The current requirement for individual schools or school bodies to identify products and services that serve educational purposes, as well as guaranteeing the safety and privacy of children, is unrealistic and unachievable.[30] EdTech products and services are complex, offered by many different providers, and usually include a myriad of tools, from MIS, tools for teaching, learning, safeguarding and administration, as well as other tech that is not specifically designed for schools but is used in school setting. Schools are also being required to make a judgement on hardware and software, and the interoperability and compatibility of one with the other.

Both the time and expertise required by schools to assess EdTech's educational value, data protection and safety is a barrier to making sound choices.[31] Introducing certification would also give market visibility to well-performing products that have been peer reviewed, and offer real benefits to children and schools.

Current DfE-approved frameworks for schools' ICT procurement primarily concern legal procurement requirements (ensuring a competitive tender process, costs and value for money, quality and service indicators, and pre-agreed Terms and Conditions deemed safe or favourable for customers).[32] Insufficient stress is placed on demonstrable educational benefits. Nor do they prioritise or appear to offer up-to-date requirements of children's data protection. While they cover some aspects of certain products and services used for teaching and learning, such as Microsoft 365 and Google Workspace for Education, and safeguarding software, such as CPOMS,[33] they do not cover other popular products such as ClassDojo,[34] MyMaths or Times Tables Rock Stars, or the various EdTech available at no financial cost.

Other assessment frameworks are in operation, but these use variable criteria and are not comprehensive. These include: (i) DfE's effectiveness assessment of EdTech used in schools, based on the value of EdTech as perceived by teachers;[35] (ii) the Education Endowment Foundation (EEF), which considers education benefit and technical security;[36] and (iii) ad hoc academic research.[37]

[30] As identified by the Centre for Data Ethics in 2021, the EdTech market is difficult for both vendors and educators to navigate due to the lack of centralised or standardised processes for EdTech procurement; see DfE (2021). ; see also Winchester (2023) for concerns about fairness in this complex market.
[31] Recognising this, the Welsh government has designed its own standardised EdTech product used in schools across the country. Welsh Government (2023a, 2023b).
[32] These DfE frameworks are voluntary and intended to relieve schools of individually vetting the provisions of each EdTech product. See DfE (2022a).
[33] Everything ICT (2022).
[34] In 2021, ClassDojo was downloaded 849,000 times. In summer 2022, our nationally representative survey of 1,014 6- to 17-year olds found that 18% use ClassDojo at school. Without reliable evidence of risks or benefits, it is difficult for schools to make an informed decision about using ClassDojo. See also Revolution Professional (2019).
[35] Walker et al (2022).
[36] Stringer et al (2019).
[37] Admiraal et al (2020), Darvishi et al (2022), McKnight et al (2016).

The DfE has a set of digital and technology standards,[38] but these do not yet cover software for teaching and learning.[39] Like the NHS, the DfE itself is required to apply the gov.uk Service Standards, and these could provide the basis of any future guidance and certification schemes for EdTech quality assurance.[40]

What is required is a standardised comprehensive framework for assessing and approving EdTech regarding its:

- educational values and benefits
- opportunity costs or risks (including in relation to future education or employment)
- usability and accessibility
- interoperability
- data protection and privacy
- security.

The lack of a standard framework in education contrasts with current good practice in health and social care (see Box 6).

Box 6: Standard assessment criteria for digital technologies in health and social care[41]

In health and social care, digital technologies to be prescribed to patients or users must be assessed against standardised criteria for clinical safety, data protection, security, interoperability, usability and accessibility. These Digital Technology Assessment Criteria (DTAC) for health and social care are 'designed to be used by healthcare organisations to assess suppliers at the point of procurement or as part of a due diligence process, to make sure digital technologies meet [the health and social care] baseline standards'.[42] DTAC brings together in a coherent and comprehensive framework the legislation, regulations and good practice relevant to the common components of a diverse range of digital technologies used in health and social care.

[38] DfE (2022).
[39] DfE (2019) offered some considerations for schools thinking of using cloud-based services, and referred to the National Cyber Security Centre's guidance on basic cybersecurity considerations.
[40] DfE (2022b); GOV.UK (n.d.).
[41] The assessment criteria used in the health and social care sector (NHS England – Transformation Directorate, 2022) offer a useful model for digital technologies that can be adapted for schools' and colleges' decision making about technology uses. Currently, technology assessment in education is fragmented, being carried out by different organisations without harmonised frameworks. The DfE's evaluation of EdTech implementation in schools and colleges spans a broader range of technologies, including 3D printers, E-readers (for learners), MIS, one-to-one learner devices and collaborative online platforms. However, the evaluation criteria focus on the processes of selecting, trialling and implementing the technologies (DfE, 2022d). The impact or effectiveness assessment of EdTech used in schools is based on schools' perceived value of EdTech (Aston et al, 2022; ImpactEd Ltd, 2022; Walker et al, 2022). The *Digital and Technology Standards in Schools and Colleges* set out by the DfE do not cover EdTech platforms, applications, products or services used for teaching and learning, and nor do they include MIS (DfE, 2022f). The majority of EdTech assessments carried out by the Education Endowment Foundation (EEF) (Stringer et al, 2019) and academics (Admiraal et al, 2020; Darvishi et al, 2022; McKnight et al, 2016) tend to focus on learning EdTech.
[42] NHS England – Transformation Directorate (2022).

2.2. Certification criteria for all EdTech used in schools

Certification criteria should include compliance with relevant legislation, regulations for data protection and security, and good practices of interoperability and risk–benefit calculation. The DfE setting out and publishing accreditation requirements for EdTech would provide clear guidance on the standards to be met and a clear mechanism of proving this to schools, reducing the burden on schools and creating a level playing field in industry.

The certification criteria should be applied to all EdTech used in schools for teaching, learning, administration and safeguarding:

1. **Full compliance with the UK AADC.**[43]

2. **Compliance with privacy and security standards (e.g., ISO/IEC 27032,**[44] **ISO/IEC 27001 and ISO/IEC 27010**[45]**)**, proportionate to the risks of the data processing, and with the UK government's accessibility requirements (e.g., WCAG 2.1[46])**.**

3. **Automatic application and extension of high privacy protection by EdTech to any resources used or accessed as part of a user's digital learning journey by default and design** (needed where EdTech allows users to access products or services with different or inferior privacy protection).[47]

4. **Biometric data**[48] is sensitive personal data and must not be processed unless one of the conditions for processing special category data applies.[49] Where biometric data is processed, it requires strong safeguards and cybersecurity.[50] In educational settings, children, parents and caregivers must be explicitly notified of the processing of biometric data and given opportunities to provide informed consent.[51] Children and parents must also be able to object to the processing and withdraw the consent given at any time.

[43] Standard 11 (parental controls) in the AADC applies to EdTech and Safety Tech used in schools; Standard 14 (connected toys or devices) applies to any internet-connected device.
[44] ISO/IEC 27032 also prescribes technical requirements for 'interoperability between different stakeholders' (ISO, 2012). By complying with cybersecurity standards, digital providers, including EdTech, will have to address interoperability, because without interoperability the data risk being compromised during an exchange, and therefore the data integrity aspect of security is lost.
[45] ISO/IEC 27010 focuses on security in relation to the exchange and sharing of sensitive information (ISO, 2015).
[46] Web Content Accessibility Guidelines (WCAG 2.1) level AA is the minimum requirement for digital services to meet the UK government's accessibility requirements (Accessibility and Assisted Digital, 2021). The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018 require digital technologies used by publicly funded bodies to meet the government's accessibility requirements.
[47] This can be achieved by ensuring that linked services create isolated 'user space' environments to which privacy protection policies can be applied. 'User space' environments are like isolated containers that act like shields protecting the items (e.g., accounts and devices) operating within the containers by filtering interactions between the items in the containers and other entities (e.g., other containers, operating systems components) outside the containers based on predetermined rules (e.g., privacy policies) (see Santos et al, 2017, pp 411–13).
[48] Protection of Freedoms Act 2012, Section 26.
[49] The conditions for processing special category data under Article 9 of the UK GDPR (which are separate to the lawful basis for processing personal data under Article 6 of the UK GDPR) include: (1) explicit consent; (2) employment, social security and social protection (if authorised by law); (3) vital interests; (4) not-for-profit bodies; (5) made public by the data subject; (6) legal claims or judicial acts; (7) reasons of substantial public interest (with a basis in law); (8) health or social care (with a basis in law); (9) public health (with a basis in law); and (10) archiving, research and statistics (with a basis in law).
[50] For a useful explanation of how this applies in schools see: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv/case-study
[51] As prescribed in the Protection of Freedoms Act 2012, Section 26.

5. **Meaningful distinction between factual personal data and inferred or behavioural judgements about children:** Maintain a separation between these types of data and do not automate linkages, construct profiles or conduct learning analytics in ways that cannot be disaggregated. Where data are inferred, a clear and transparent account of how the analysis is constructed should be available to the certification body and schools to ensure that behavioural or educational inferences are meaningful and contestable.

6. **Opportunities to review and correct errors in the data held about children:** Proactively provide prominent, child-friendly and accessible tools for children, parents and caregivers to understand what data is held about the child, enable children and caregivers to review and correct any errors in education records about the child, and provide redress if the errors result in harm.

7. **Vulnerability disclosure:** Provide prominent and accessible pathways for security researchers and others to report any security vulnerabilities of the tools and establish an internal process to act on the reported vulnerabilities in a timely manner.

8. **Evidence-based educational benefits:** Provide up-to-date peer-reviewed evidence of the benefits of EdTech products, using robust methodologies, produced by independent experts free from any conflict of interest.[52]

9. **In-product research:** Education data used for R&D by the EdTech provider must meet high ethical and child rights standards. It should not be routine or conducted on children's education data without meaningful informed consent.

10. **Linked services:** Ensure that any service linkages and plug-ins, including in-app purchases made accessible in EdTech products or services, meet these standards.

A certification scheme for EdTech would support schools to identify products that protect children's data rights and provide clear pedagogical, safeguarding or administrative benefits while enabling EdTech providers to communicate the evidence-based benefits of their products and compliance with relevant standards and regulations. Collectively, the certification would build trust in EdTech and boost adoption. Therefore, the DfE, with the support of the regulator and the commercial certification sector, should provide a seamless system in which EdTech products are certified to meet recommended criteria.

The assessment of conformity with the certification scheme, including the above criteria, should be performed by organisations recognised and accredited by the United Kingdom Accreditation Service (UKAS) as competent and impartial to audit EdTech products or services and issue certification.[53] An example of an accredited certification scheme is the Age Appropriate Design Certification.[54]

[52] Evidence should be evaluated against clear pedagogic expectations, using open science principles of transparency, accessible knowledge, open data, contestation and validation by third parties, and include a determination that the benefits are proportionate to any risks to children's rights.
[53] UKAS (2022).
[54] Age Check Certification Scheme Ltd (2021)

Action 5: The DfE, in consultation with relevant expert advice, the ICO, academia and children, should introduce an evidence-based certification scheme to cover the use of EdTech in schools based on the 10 criteria, and encourage EdTech certification uptake.

Action 6: UKAS should assess and accredit certification bodies to audit and certify EdTech products or services for compliance with the certification criteria.

Action 7: The DfE should set out the educational purposes that EdTech may serve, and maintain an independent evidence base to support this.

Action 8: The DfE should introduce a requirement for schools to conduct a Child Rights Impact Assessment (CRIA) if they choose to use an EdTech product or service that fails to meet the 10 certification criteria specified in Action 5, where it has the potential to impact fundamental rights, updating the 2022 *Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges*.[55]

3. Develop trusted data infrastructure(s) for research, business and government that serve the best interests of children and the wider educational community

Research and innovation based on de-identified data, including that based on inter-agency public service datasets, is valuable for identifying problems affecting children's development and learning outcomes. It also opens tremendous opportunities for better targeted solutions.[56] Research and innovation can also help us understand educational effectiveness and outcomes.

However, much of the data processed from children in education is unavailable to or under-used by researchers. Meanwhile, commercial companies are harvesting data at scale, over which there has been little or no public debate over whether or how education data, which arguably belongs to the children and/or the education sector, collected but processed by private companies, could be included accessed in the public interest.

In fact, this conversation has not yet established what data are of interest, to whom, how data collected from children in education should be held, and who should have control over and/or access to it, what the rules of engagement with the data should be – and perhaps most importantly, what benefits could accrue to children in the future and the present from making such data available to the research and governance communities in education, but perhaps also in health, innovation and beyond. Meanwhile, children's data is widely

[55] See DfE (2022e).

[56] Data processing in schools is governed by the UK DPA 2018 and the UK GDPR. The census data that schools process from children forms part of the National Pupil Database (NPD), which is operated by the DfE and can be linked to other datasets. Access to use the NPD held by a public authority, in this case, the DfE, is governed by the Digital Economy Act (DEA) 2017. Chapter 5 of the DEA 2017 permits the sharing of publicly held data for research purposes under strict conditions, for example that personally identifiable data is de-identified, with minimal risks of reidentification, before sharing, and that the 'research' for which the data is shared is accredited (following criteria published by the UK Statistical Authority) under Section 71. Pursuant to these requirements, the DfE declares compliance with the Five Safes Framework, originated by the Office for National Statistics (ONS), to address the risks of identification of individual data subjects, security and access control over the data (Ritchie, 2017, p 2). The Five Safes Framework is widely used internationally as a standard for providing safe data access for statistical research (UK Data Service, 2021).

available to the commercial tech sector.[57] This must be resolved before data sharing can be trusted.

To realise the social and economic benefits of data to serve children's best interests, a trusted data-sharing infrastructure is needed which is:

- secure
- respects individuals' confidentiality
- complies with data protection and privacy laws
- ensures data is used solely for permitted purposes
- is in the public interest and/or in the best interests of the child.

Stakeholders should be able to identify clearly:

- what data is being collected
- for what purpose(s)
- who owns or holds the data
- where the data is stored
- why and with whom it is shared
- who else is involved in the data sharing
- how it could impact on the child's data footprint in the future.

3.1. Determine which data should be publicly accessible

Commercial companies have already gained access to education records held by the DfE for 'accredited research purposes in the public good'[58] but do not reciprocate, often citing Intellectual Property (IP) or commercial reasons for not allowing researchers and civil society to access the wealth and variety of education data collected from children and held by private EdTech companies.[59]

Access to and use of private education data to generate knowledge and insights in the public interest needs to be more widely available and better managed to ensure compliance with data protection and privacy laws and respect for children's rights. Research funding bodies could support research strategies with competitive funding to create educational benefits from pupil data, not only to inform public policy, but also to adequately audit, assess and provide independent oversight of EdTech products and services and their impact. Developing a mechanism(s) for access interoperability and standardisation of data systems should be fundamental to create understanding and trust.

[57] Much of the data schools must collect by law (Section 537A of the Education Act 1996) is 'analogue' (age, address, educational record etc.), but EdTech has the capacity to create more detailed, comparative, real-time and collective data (e.g., which children learn more quickly at a certain time of day, whether movement increases memory, etc.). This data is available to commercial EdTech, but it does not contribute to the public understanding of how to improve educational outcomes or the wellbeing of children.

[58] See DfE (2022c) and Day et al (2022).

[59] For example, schools and education authorities are currently assessing the impact of large language models trained on data including that obtained through EdTech in schools. It is likely that schools will have to invest in commercial software provided by those who have already collected the training data through their plagiarism software, as in the case of ChatGPT.

Well thought-through systems of data stewardship have the potential to revolutionise outcomes for children's education. However, to unlock the value of this data in the public interest, and thus enable beneficial uses of privately held data obtained via publicly funded education, a commitment and motivation to share anonymised data for research and public service delivery is required. For example, requiring EdTech to be based on open source and open data principles and being interoperable could result in larger data pools for both UK businesses and researchers, leading to increased innovation and better outcomes for children.[60]

Action 9: The DfE should consult on an operational model of education data sharing, to include data processed by EdTech, in the public interest.[61]

3.2. Develop a clear framework for data access

Publicly held education data are, in principle, governed by clear regulatory frameworks and access control mechanisms. However, the onward data sharing of publicly held education databases does not consistently apply data access control mechanisms, and nor does it always comply with data protection regulations. Such systems must be subject to agreed governance criteria, and ensure the understanding of parents, caregivers, teachers and children on the implications of data sharing and research, and there must be a high level of oversight and clear redress mechanisms when things go wrong.

In terms of publicly held education data, the DfE holds responsibility for the creation, maintenance and onward use of datasets such as the National Pupil Database (NPD), a database that holds significant amounts of personal data about schoolchildren, and other databases of children's educational records. Access to these data is generally managed by the Office for National Statistics (ONS), which is mandated to operate secure data-sharing facilities in accordance with the Five Safes Framework (see Box 7).

Box 7: The Five Safes Framework

According to the UK Data Service, the Five Safes Framework is commonly used by UK secure labs, including the Office for National Statistics (ONS), to allow approved researchers to access personal data, including sensitive data, without compromising data subjects' privacy. The framework comprises five principles:

1. 'Safe data' guards against confidentiality concerns.
2. 'Safe projects' require data controllers to ensure and approve appropriate, lawful and ethical uses of data for the public good.
3. 'Safe people' refers to trusted data users – accredited and authorised researchers.
4. 'Safe settings' means that the facilities that provide research access to data have capabilities to limit unauthorised use of data.
5. 'Safe outputs' ensures that the research outputs maintain the confidentiality of the data subjects.

Individually, these principles reduce the risks of misuse, unauthorised access or unauthorised use of sensitive data. Applied in combination, they provide assurance of safe data sharing and use.

[60] This would be consistent with the approach taken by UNICEF (2019).
[61] This recommendation is modelled on the French legal provision in Article 53-1 of the amended Ordinance No. 2018-65 of 29 January 2016, relating to concession contracts (République Française, 2019).

However, the Five Safes Framework is inconsistently applied by the DfE in its decisions and data-sharing practices, and it has been criticised for allowing media, gambling companies and others access to children's data. In a 2020 audit, the ICO found that alternative routes to accessing these data directly from the DfE violated the Five Safes Framework and raised data protection issues (see Box 8).[62]

Box 8: The DfE is reprimanded for misuse of education data

The ICO's (2022a) investigation revealed that gambling companies had been profiting from the Learning Records Service, a database owned and run by the DfE. A training company had originally been granted access to children's personal data for the purpose of providing training. This training company then reused this data for a different purpose, namely to provide commercial age verification services to gambling companies. Therefore, the ICO found against the DfE for failing to comply with UK GDPR Article 5(1)(a) and Article 5(1)(f), which require data controllers to protect against 'the unauthorised processing by third parties' and safeguard the confidentiality of data subjects.

Fulfilling the Five Safes Framework is a minimum requirement, and data access control practice should also include audit of the actual data use to ensure that it is consistent with the purpose of data use given in the data access application. It should also introduce a clear redress procedure for children whose education records have been exploited.

Action 10: The ICO should reinforce the DfE's application of the Five Safes Framework with a robust audit system to ensure that the DfE's data sharing of children's education records adheres to data protection laws and the Five Safes Framework.

Action 11: The DfE (as data controller) should set up an easily accessible system of redress for children whose data have been exploited.

Action 12: The DfE should fund research based on its databases of children's educational records and other publicly held datasets to create educational benefits either directly or through research funding bodies.

3.3. The future of access to education data

Governance methods that promote the safe and seamless sharing of data will continue to evolve, and there may be new methods that can empower schools, parents, caregivers and children to have more of a say over who can access what education data or for what purpose, particularly in relation to private organisations.

The sandbox principle, where tech products and processes can be tested in circumstances that are transparent and safe (for both companies and the child), is popular with businesses, regulators and consumers. We suggest a pilot project with several sandbox schools and a

[62] Day et al (2022).

mix of EdTech products to trial these ideas to see what can be learned by sharing data held by business for rights-respecting uses of education data in the future (see Box 9).

Box 9: Born in Bradford project

The Born in Bradford (BiB) project demonstrates the potential and actual benefits of confidential data linkages across administrative records of citizens, including children living in Bradford. Through frequent engagement with children and their families, researchers were able to obtain informed consent to ethically continue routine data linkage (e.g., health, social care and education records) for longitudinal studies of over 30,000 Bradfordians. To maintain the confidentiality of data and data subjects, the BiB research team use a 'non-unique personal identifier' to match the data of an individual in the education system with the same individual's health records, with minimal risk of reidentification. The cross-comparison of the health and education datasets revealed new insights into how health problems – such as ophthalmic deficit – impede the development of children's reading skills. This insight resulted in a better-targeted solution for improving the reading skills of those who have fallen behind, by getting children properly prescribed glasses.[63]

Emerging models of data stewardship are experimenting with decentralised data governance structures, reliance on trusted intermediaries (independent third parties) and data trusts. For example, a data trust allows for data subjects to provide their data to a trusted intermediary with built-in privacy controls, who would allow access to the collective pool of data to appropriate third parties to use in ways that benefit the data subjects.[64] Examples of existing data trust models include the Databox project[65] and Mydex CIC.[66]

Insights drawn from education data and digital technologies used to deliver education (EdTech) promise great benefits to children and their learning experience, enhancing children's best interests. These include:[67]

- tracking aggregated student progress across settings to target interventions
- helping teachers to evaluate students' progress against national standards
- early identification of special educational needs and disabilities to guide support
- personalised learning to support educational outcomes
- improving the discovery of educational content by analysing user engagement
- helping schools improve their services and processes and guide resource allocation
- identifying safeguarding needs to support child protection
- promoting public health benefits by analysing the needs of vulnerable children
- researching and documenting the benefits of educational interventions
- defining and optimising algorithms that can improve children's outcomes
- combining education data with other datasets to produce new insights

[63] This example is adapted from Mon-Williams et al (2022).
[64] Such a model would require significant advances in a number of areas: improvements in technical interoperability and data readability across systems, better means of compelling data controllers to provide ongoing data extracts, clarity on the role of parents in managing their child's data, a range of trusted intermediaries to act as the data trustee, and better data literacy among schools, parents and caregivers and children so that they can realise the value of the data trust.
[65] SysAL (n.d.).
[66] Mydex (n.d.).
[67] Livingstone et al (2021).

Action 13: The DfE should fund and work with the ICO to set up sandboxes for privacy and child rights-respecting data trust models for education data, and experiment with how these models can be effectively integrated into the UK education ecosystem to facilitate access to and usage of privately held education data in the public interest.[68]

Contingencies

The lack of action on education data is in part because of a lack of understanding of the problem and its significance, and in part because those grappling with the problem (school leaders, parents and caregivers) often have the least access to resources and information. So, while the actions set out in this blueprint would usher in a new framework of protections, there are some contingencies to make the environment ready to accept and build on these changes.

Around the globe governments and regulators struggle with both privacy and clarity of what is and isn't good EdTech. There is clearly a first mover advantage in setting out fair terms and measurement metrics on what works that has the potential to make an impact on the market, which is currently worth US$4.68 billion to the UK.[69]

Political narratives emphasise the benefits of these changes, which, in turn, requires developing expertise within the DfE, Department for Science, Innovation and Technology and ICO on this issue. It also means that EdTech needs to be considered in wider digital regulation, for example, online safety, trade, data flow and other relevant policy areas.

At the same time, Ofsted needs to ensure that it has a nuanced understanding of the role of EdTech in schools. It is not fair or right to assume that the use of EdTech in a school setting is automatically beneficial. Closer attention must be paid to evidence of the chosen EdTech being fit for purpose and well used, as well as privacy-preserving. When it is implemented, consideration must be given to whether an EdTech product has gained the certification outlined above.

Finally, and perhaps most importantly, the government must find the resources to support the proposed changes.

Afterword

Across the blueprint, two consistent themes emerge: the need for better data management with a focus on children's privacy and a resolution to the problem that society is prevented from accessing children's data to benefit from the insights it might bring. In the ever-evolving digital world the blueprint cannot hope to be the last word. But its 13 actions do represent a giant leap towards eliminating the egregious, streamlining the management of data in schools, and ensuring children's data is processed in their best interests.

[68] This project was pioneered in France in 2022 (CNIL, 2022).
[69] See GlobalData (2022).

Annex 1: Recent instances of data protection risks

The UK is not alone in being exposed to data and other governance risks in EdTech (see Table 1). These risks undermine children's rights and life prospects. There are lessons to be learned from decisions made in other jurisdictions to mitigate these risks. For example, the adoption of AI-driven systems can bring benefits but could expose users to misuse of personal data and lead to unforeseen consequences.[70]

Table 1. Data protection and other risks concerning EdTech identified by jurisdiction

Date	Jurisdiction	Finding and decision on risk in EdTech use
March 2021	Netherlands	Multiple high data protection risks identified in Google education products resulting in a negotiated agreement[71]
May 2022	International	Human Rights Watch reported 49 governments had recommended unsafe products for education purposes during the COVID-19 pandemic; 145 of these had surveillance capabilities to monitor children while learning[72]
July 2022	Denmark	The Data Protection Authority bans the use of Google Workspace and Chromebooks in Helsingør, having identified high data protection risks concerning lack of transparency in data processing and use and missing or problematic privacy controls[73]
August 2022	UK	The Digital Futures Commission's review of Google Classroom and ClassDojo identified data protection risks
August 2022	Oakland, USA	Remote Proctoring, used to monitor students and their homes during exams, was found to have violated privacy laws[74]
November 2022	England	The ICO reprimanded the DfE for misuse of education data[75]
November 2022	France	The French Ministry of Education urged schools to stop using the free versions of Google Workspace for Education and Microsoft Office 365[76]
January 2023	Australia	Redesign of testing deemed critical and a likely return to pen-and-paper exams owing to plagiarism fears around ChatGPT[77]
January 2023	New York, USA	ChatGPT banned from all public school devices[78]

[70] To take a recent instance, ChatGPT could be used to enhance education, but at the same time it can provide inaccurate, discriminatory or biased responses and lead to cheating and plagiarism and may require legislative change.
[71] Nas & Terra (2021a, 2021b).
[72] Human Rights Watch (2022).
[73] The European Data Protection Board (EDPB, 2022) noted that this was likely to apply to other municipalities, and is finalising several relevant cases.
[74] Hawkins (2022).
[75] See ICO (2022b) and Box 8 in Section 3.2 of this blueprint.
[76] Kundaliya (2022).
[77] Cassidy (2023).
[78] Rosenblatt (2023).

Annex 2: Complete list of actions

Action	Relevant legislation	Acting authority
Best interests of the child		
Action 1: The UNCRC and General Comment No. 25 should be explicitly referenced in all existing and future law, policy and practice relating to children's education data	Data Protection and Digital Information Bill 2022 (add the clause to reference the UNCRC and General Comment No. 25: In all parts of this Bill, the best interests of the child shall be a primary consideration in all actions involving the processing of data from or about a child or children)	Parliament
Data protection		
Action 2: Age Appropriate Design Code (**AADC) application.** The government should use the Data Protection and Digital Information Bill 2022 to clarify that all EdTech that process data about children must meet the data protection and privacy baseline provided by the AADC	Data Protection and Digital Information Bill 2022 AADC	Government
Action 3: **Data protection compliance.** The ICO should develop an education-specific checklist to identify the controller in practice. Where there is a lawful basis for EdTech providers to become joint controllers, it must be possible for each party to fulfil their data controller responsibilities proportionate to the volume, variety and usage of the data they process without overburdening the other. In all cases, responsibilities must not be put on to those who cannot in practice fulfil them.	Data Protection and Digital Information Bill 2022 Data Protection Act 2018 UK General Data Protection Regulation (GDPR) AADC	Government/ICO to ensure better resourcing and effective enforcement
Standard contractual clauses		
Action 4: The DfE should develop, with the support of the ICO and/or Crown Commercial Service, standard contractual clauses for schools to insert into their contracts with EdTech providers. These should restrict EdTech's data processing to the processing purposes that schools choose and can reasonably audit	UK Government Service Standard[79] (Principles 10 and 11)	DfE (or Crown Commercial Service)
Certification		

[79] DfE (2022b) and GOV.UK (n.d)

Action 5: The DfE, in consultation with relevant expert advice, the ICO, academia and children, should introduce an evidence-based certification scheme to cover the use of EdTech in schools based on the 10 criteria, and encourage EdTech certification uptake	Policy	DfE
Action 6: UKAS should assess and accredit certification bodies to audit and certify EdTech products or services for compliance with the certification criteria	Conformity assessment and accreditation policy[80]	UKAS
Guidance		
Action 7: The DfE should set out the educational purposes that EdTech may serve, and maintain an independent evidence base to support this	Policy	DfE
Action 8: The DfE should introduce a requirement for schools to conduct a child rights impact assessment (CRIA) if they choose to use an EdTech product or service that fails to meet the 10 certification criteria specified in Action 5, where it has the potential to impact fundamental rights, updating the 2022 *Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges*	Policy	DfE
Data sharing		
Action 9: The DfE should consult on an operational model of education data sharing, to include data processed by EdTech, in the public interest	*Data Sharing Governance Framework* (Central Digital & Data Office, 2022)	DfE
Action 10: The ICO should reinforce the DfE's application of the Five Safes Framework with a robust audit system to ensure that the DfE's data sharing of children's education records adheres to data protection laws and the Five Safes Framework	Digital Economy Act 2017 UK GDPR *Data Sharing Governance Framework* (Central Digital & Data Office, 2022)	The ICO to audit the DfE's data practices
Action 11: The DfE (as data controller) should set up an easily accessible system of redress for children whose data have been exploited	UK GDPR	DfE
Action 12: The DfE should fund research based on its databases of children's educational records and other publicly held datasets to create educational benefits either directly or through research funding bodies.	Digital Economy Act 2017	DfE
Action 13: The DfE should fund and work with the ICO to set up sandboxes for privacy and child rights-respecting data trust models for	UK GDPR Data Protection and Digital Information Bill –	DfE and ICO

[80] See Office for Product Safety and Standards & Department for Business, Energy Industrial Strategy (2012).

education data, and experiment with how these models can be effectively integrated into the UK education ecosystem to facilitate access to and usage of privately held education data in the public interest	potential to use the provision for the Secretary of State to regulate and protect the interests of children coupled with use/reuse of data for scientific research (Article 4, UK GDPR, amended in new Chapter 8A)	

References

5Rights Foundation. (2022). 5Rights celebrates the first anniversary of the Age Appropriate Design Code. https://5rightsfoundation.com/in-action/5rights-celebrates-the-first-anniversary-of-the-age-appropriate-design-code.html

Accessibility and Assisted Digital. (2021). Making your service accessible: An introduction. www.gov.uk/service-manual/helping-people-to-use-your-service/making-your-service-accessible-an-introduction#meeting-government-accessibility-requirements

Admiraal, W., Vermeulen, J., & Bulterman-Bos, J. (2020). Teaching with learning analytics: How to connect computer-based assessment data with classroom instruction? *Technology, Pedagogy and Education*, *29*(5), 577–91. https://doi.org/10.1080/1475939X.2020.1825992

Aston, J., Davies, E., Guijon, M., Lauderdale, K., & Popov, D. (2022). *The Education Technology Market in England: Research Report*. Department for Education, November. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1117067/Edtech_market_in_England_Nov_2022.pdf

BESA (British Educational Suppliers Association). (no date). Key UK education statistics. www.besa.org.uk/key-uk-education-statistics

Cassidy, C. (2023). Australian universities to return to 'pen and paper' exams after students caught using AI to write essays. *The Guardian*, 10 January. www.theguardian.com/australia-news/2023/jan/10/universities-to-return-to-pen-and-paper-exams-after-students-caught-using-ai-to-write-essays

Central Digital & Data Office. (2022). *Data Sharing Governance Framework*. www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework

Centre for Data Ethics and Innovation. (2021). *AI Barometer Part 5 – Education*. www.gov.uk/government/publications/ai-barometer-2021/ai-barometer-part-5-education

Children Act. (1989). https://www.legislation.gov.uk/ukpga/1989/41/contents

Children Act. (2004). https://www.legislation.gov.uk/ukpga/2004/31/contents

CNIL (Commission Nationale Informatique & Libertés). (2022). EdTech 'sandbox': The CNIL supports 10 innovative projects. 25 May. www.cnil.fr/en/edtech-sandbox-cnil-supports-10-innovative-projects

Darvishi, A., Khosravi, H., Sadiq, S., & Gašević, D. (2022). Incorporating AI and learning analytics to build trustworthy peer assessment systems. *British Journal of Educational Technology*, *53*(4), 844–75. https://doi.org/10.1111/bjet.13233

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

Day, E. (2021). *Governance of Data for Children's Learning in UK State Schools*. Digital Futures Commission and 5Rights Foundation. https://digitalfuturescommission.org.uk/beneficial-uses-of-education-data

Day, E., Pothong, K., Atabey, A., & Livingstone, S. (2022). Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech. *Learning, Media and Technology*, 1–15. https://doi.org/10.1080/17439884.2022.2152838

DfE (Department for Education). (2019). Moving your school to the cloud. 3 April. www.gov.uk/government/publications/moving-your-school-to-the-cloud/moving-your-school-to-the-cloud

DfE. (2021). *Independent Report - AI Barometer Part 5: Education*. https://www.gov.uk/government/publications/ai-barometer-2021/ai-barometer-part-5-education

DfE. (2022a). All frameworks: ICT. https://find-dfe-approved-framework.service.gov.uk/list#category-ict

DfE. (2022b). *Apply the Service Standard in DfE*. https://apply-the-service-standard.education.gov.uk/

DfE. (2022c). How DfE shares personal data. www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

DfE. (2022d). *Implementation of Education Technology in Schools and Colleges, Research Report*. CooperGibson Research, October. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1107808/Implementation_of_education_technology_in_schools_and_colleges.pdf

DfE. (2022e). *Keeping Children Safe in Education 2022: Statutory Guidance for Schools and Colleges*. 1 September. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101454/Keeping_children_safe_in_education_2022.pdf

DfE. (2022f). *Meeting Digital and Technology Standards in Schools and Colleges.* 23 March. www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges

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

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

EDPB (European Data Protection Board). (2022). The Danish DPA imposes a ban on the use of Google Workspace in Elsinore municipality. 19 July. https://edpb.europa.eu/news/national-news/2022/danish-dpa-imposes-ban-use-google-workspace-elsinore-municipality_en

Everything ICT. (2022). Over 180 suppliers covering every area of ICT. www.everythingict.org/suppliers

Fowler, A. (2013).Lightbeam for Firefox: Privacy education for users & open data for publishers. Dist://ed Blog, 25 October. https://blog.mozilla.org/en/mozilla/lightbeam-for-firefox-privacy-education-for-users-open-data-for-publishers

GlobalData. (2022). United Kingdom (UK) EdTech Market Summary, Competitive Analysis and Forecast, 2021–2026. 30 September. www.globaldata.com/store/report/uk-edtech-market-analysis

GOV.UK. (no date). Service Standard. www.gov.uk/service-manual/service-standard

Hawkins, S. (2022). Remote testing 'room scans' violate Fourth Amendment, judge says. Bloomberg Law, 23 August. https://news.bloomberglaw.com/privacy-and-data-security/remote-testing-room-scans-violate-fourth-amendment-judge-says

Hooper, L., Livingstone, S., & Pothong, K. (2022). *Problems with Data Governance in UK Schools: The Cases of Google Classroom and ClassDojo*. Digital Futures Commission

and 5Rights Foundation.. https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf

Human Rights Watch. (2022). *'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments that Endorsed Online Learning During the COVID-19 Pandemic.* www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

ICO (Information Commissioner's Office). (2020). *Age Appropriate Design: A Code of Practice for Online Services*. https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf

ICO. (2021). Age Appropriate Design Certification Scheme (AADCS). *Age Check Certification Scheme Ltd*. https://ico.org.uk/for-organisations/age-appropriate-design-certification-scheme-aadcs

ICO. (2022a). *Children's Code: Best Interests Framework*. https://ico.org.uk/for-organisations/childrens-code-hub/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/children-s-code-best-interests-framework/

ICO. (2022b). Department for Education warned after gambling companies benefit from learning records database. 6 November. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/11/department-for-education-warned-after-gambling-companies-benefit-from-learning-records-database

ICO. (2022c). ICO could impose multi-million pound fine on TikTok for failing to protect children's privacy. 26 September. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-could-impose-multi-million-pound-fine-on-tiktok-for-failing-to-protect-children-s-privacy

ICO. (2022d). *Regulating the Digital Economy*. https://ico.org.uk/media/about-the-ico/disclosure-log/4019846/ic-151664-d5q4-9-rg048-regulating-the-digital-economy-redacted.pdf

ICO. (2022e). *Guide to Data Protection*. https://ico.org.uk/media/for-organisations/guide-to-data-protection/introduction-to-dpa-2018-1-0.pdf

ImpactEd Ltd. (2022). *EdTech Demonstrator Programme (Phase 2 – 2021 to 2022) Evaluation: Research Report*. Department for Education, November. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1115740/EdTech_Demonstrator_Impact_Evaluation_Report_November_2022.pdf

ISO (International Organisation for Standardisation). (2012). *Information Technology – Security Techniques – Guidelines for Cybersecurity*. ISO/IEC 27032: 2012(E). https://webstore.iec.ch/preview/info_isoiec27032%7Bed1.0%7Den.pdf

ISO. (2015). *Information Technology – Security Techniques – Information Security Management for Inter-Sector and Inter-Organisational Communications*. ISO/IEC 27010:2015. www.iso.org/standard/68427.html

Kundaliya, D. (2022). France bans Office 365 and Google Workspace in schools: Country has concerns over competition and regulation. Computing, 21 November. www.computing.co.uk/news/4060509/france-bans-office-365-google-workspace-schools

Livingstone, S., Atabey, A., & Pothong, K. (2021). *Addressing the Problems and Realising the Benefits of Processing Children's Education Data: Report on an Expert Roundtable*. Digital Futures Commission, 5Rights Foundation.

https://digitalfuturescommission.org.uk/wp-content/uploads/2021/11/Roundtable-report-25112-final.pdf

McKnight, K., O'Malley, K., Ruzic, R., Horsley, M.K., Franey, J.J., & Bassett, K. (2016). Teaching in a Digital Age: How Educators Use Technology to Improve Student Learning. *Journal of Research on Technology in Education*, *48*(3), 194–211. https://doi.org/10.1080/15391523.2016.1175856

Mon-Williams, M., Elshehaly, M., & Sohal, K. (2022). Connected Data for Connected Services that Reflect the Complexities of Childhood. In S. Livingstone & K. Pothong (eds) *Education Data Futures: Critical, Regulatory and Practical Reflections*. 5Rights Foundation. https://educationdatafutures.digitalfuturescommission.org.uk/essays/competing-interests-in-education-data/connected-data-connected-services

Mydex. (no date). Mydex CIC helps individuals and service providers improve their handling of personal data. https://mydex.org

Nas, S. & Terra, F. (2021a). DPIA on the use of Google G Suite (Enterprise) for education. 15 July 2020 [Updated 12 March 2021]. Privacy Company. https://www.surf.nl/files/2021-06/updated-g-suite-for-education-dpia-12-march-2021.pdf

Nas, S. & Terra, F. (2021b). *Update DPIA Report, Google Workspace for Education*. Privacy Company, 2 August. www.surf.nl/files/2021-08/update-dpia-report-2-august-2021.pdf

NHS England – Transformation Directorate. (2022). Digital Technology Assessment Criteria (DTAC). https://transform.england.nhs.uk/key-tools-and-info/digital-technology-assessment-criteria-dtac

Office for Product Safety & Standards, & Department for Business and Trade. (2012). *Organisations*. https://www.gov.uk/government/organisations/office-for-product-safety-and-standards

OHCHR. (1993). Economic Exploitation of Children (Excerpted from CRC/C/20, 4th Session, 4 October 1993). https://www.ohchr.org/sites/default/files/HRBodies/CRC/Documents/Recommandations/exploit.pdf

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

République Française. (2019). Code des relations entre le public et l'administration. www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033265181

Revolution Professional. (2019). Data Protection Impact Assessment (ClassDojo). https://greenfield.dudley.sch.uk/wp/wp-content/uploads/2020/05/Data-Protection-Impact-Assessment-ClassDojo.pdf

Ritchie, F. (2017). The 'Five Safes': A framework for planning, designing and evaluating data access solutions. Data for Policy 2017: Government by Algorithm? (Data for Policy), London, 6–7 September. https://zenodo.org/record/897821

Rosenblatt, K. (2023). ChatGPT banned from New York City public schools' devices and networks. NBC News, 5 January. www.nbcnews.com/tech/tech-news/new-york-city-public-schools-ban-chatgpt-devices-networks-rcna64446

The Royal Society. (2023). Privacy enhancing technologies. 23 January. https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies

Santos, O., Muniz, J., & De Crescenzo, S. (2017). *CCNA Cyber Ops, SECFND 210-250, Official Cert Guide*. Cisco Press.

Stokel-Walker, C. (2021). Britain tamed Big Tech and nobody noticed. WIRED, 2 September. www.wired.co.uk/article/age-appropriate-design-code-big-tech

Stringer, E., Lewin, C., & Coleman, R. (2019). *Using Digital Technologies to Improve Learning: Guidance Report*. Education Endowment Foundation. https://educationendowmentfoundation.org.uk/public/files/Publications/digitalTech/EEF_Digital_Technology_Guidance_Report.pdf

SysAL (Systems and Algorithms Laboratory). (no date). Databox Project. www.imperial.ac.uk/systems-algorithms-design-lab/research/databox-project

Taylor, R. (2022). *New Approaches to Data Stewardship in Education*. 5Rights Foundation, Digital Futures Commission. https://educationdatafutures.digitalfuturescommission.org.uk/essays/rethinking-data-futures/new-approaches-data-stewardship

Turner, S., Pothong, K., & Livingstone, S. (2022). *Education Data Reality: The Challenges for Schools in Managing Children's Education Data*. Digital Futures Commission, 5Rights Foundation. https://digitalfuturescommission.org.uk/beneficial-uses-of-education-data

UK Data Service. (2021). What is the Five Safes framework? https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework

UKAS (United Kingdom Accreditation Service). (2022). Accreditation vs certification: What's the difference? www.ukas.com/accreditation/about/accreditation-vs-certification

UN (1989). *Convention on the Rights of the Child*. www.ohchr.org/en/professionalinterest/pages/crc.aspx

UN Committee on the Rights of the Child. (2021). *General Comment No 25 on Children's Rights in Relation to the Digital Environment* (CRC/C/GC/25). www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

UNICEF. (2019). *LearnIn: Shaping the Culture of Education*. https://drive.google.com/file/d/1DBfxJEvdvLUPBwrB_kmY2izufiJ3Psdn/view

Walker, M., Bradley, E., Sharp, C., Grayson, H., Lopes, G., & Chu, J. (2022). *Education Technology for Remote Teaching: Research Report*. National Foundation for Educational Research. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1116497/Education_technology_for_remote_teaching_-_research_report.pdf

Welsh Government. (2023a). *Education Wales*. https://hwb.gov.wales/

Welsh Government. (2023b). *Wales Innovates: Creating a Stronger, Fairer, Greener Wales*. https://www.gov.wales/wales-innovates-creating-stronger-fairer-greener-wales-html?&focusjump=manufacturing%20community%20to%20access%20advanced%20technologies.%0AHe#117638

Winchester, N. (2023). *Oak National Academy: Impact on the Publishing and Educational Technology Sectors*. UK Parliament. https://lordslibrary.parliament.uk/oak-national-academy-impact-on-the-publishing-and-educational-technology-sectors/