

```
box-shadow: inset 2px 2px 2px rgba(0,0,0,0.5);

doodle input:checked ~ .animate {
  /* We will set a delay so that the reveal
  -webkit-animation: horse-ride .5s step(12);
  -moz-animation: horse-ride .5s steps(12);
  animation: horse-ride .5s steps(12, end);
}

/* Imitating the reveal effect
background-position: 0 0;
-webkit-transition: all 5s cubic-bezier(0.550, 0.000, 0.000, 0.550);
-moz-transition: all 5s cubic-bezier(0.550, 0.000, 0.000, 0.550);
transition: all 5s cubic-bezier(0.550, 0.000, 0.000, 0.550);
}

@-webkit-keyframes horse-ride {
0% { background-position: 0 0; }
100% { background-position: -804px 0; }
}
```

# Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo

## The Digital Futures Commission

The Digital Futures Commission (DFC) is an exciting research collaboration of unique organisations that invites innovators, policymakers, regulators, academics and civil society to unlock digital innovation in the interests of children and young people. It seeks to put the needs 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 innovation is reconfiguring children's lives to reimagine the digital world in value-sensitive ways that uphold their rights and take practical steps to meet their needs.

The DFC research team, led by Professor Sonia Livingstone OBE, has three work streams: play in a digital world, beneficial uses of education data, and guidance for innovators. Each is informed by the voices of children and underpinned by research and outputs geared toward real-world change for children.

### Commissioners

**David Halpern**, Chief Executive, 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**, Durham University

**Professor Brian O'Neill**, Technological University Dublin

**Michael Preston**, Executive Director, Joan Ganz Cooney Center, 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**, Open Data Partners

**Adrian Woolard**, Head of BBC's Research & Development

Biographies for the commissioners are [here](#) and for the researchers see [here](#)

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

Funding: The Commission is funded by 5Rights Foundation with funding in kind from LSE.

Cover image: Photo by Ali Shah Lakhani on Unsplash.

## Contents

<b>Foreword</b> .....	<b>5</b>
<b>Acknowledgements</b> .....	<b>6</b>
<b>Executive summary</b> .....	<b>7</b>
<b>This report</b> .....	<b>13</b>
<i>The Digital Futures Commission’s EdTech survey</i> .....	14
<i>Definitions</i> .....	15
<b>An introduction to Google Classroom</b> .....	<b>16</b>
<b>An introduction to ClassDojo</b> .....	<b>18</b>
<b>Problem 1: It is near impossible to discover what data is collected by EdTech</b> .....	<b>20</b>
<i>Summary of Problem 1</i> .....	25
<i>Recommendation 1: Ensure transparency and accountability for processing children’s education data</i> .....	26
<b>Problem 2: EdTech profits from children’s data while they learn</b> .....	<b>26</b>
<i>Blurring the boundary between core and additional services expands commercial data processing</i> .....	26
<i>An experiment with Google Classroom</i> .....	28
<i>Blurring the school/home boundary expands commercial data processing</i> .....	32
<i>Summary of Problem 2</i> .....	33
<i>Recommendation 2: Ensure commercial interests in education data do not undermine children’s education and best interests</i> .....	34
<b>Problem 3: EdTech’s privacy policies and/or legal terms do not comply with data protection regulation</b> .....	<b>35</b>
<i>International challenges to EdTech’s use of children’s data</i> .....	39
<i>Insufficient purpose limitation and lack of lawful basis</i> .....	40
<i>Consent as a basis for processing educational data</i> .....	42
<i>Lack of transparency: A consequence of convoluted privacy policies and/or legal terms</i> .....	43
<i>Problematic application of the Age Appropriate Design Code to EdTech</i> .....	44
<i>Summary of Problem 3</i> .....	46
<i>Recommendation 3: Ensure that EdTech provides transparent privacy policies and legal terms for their processing of children’s education data in compliance with data protection laws</i> ....	47

<b>Problem 4: Regulation gives schools the responsibility but not the power to control EdTech data processing</b> .....	<b>48</b>
<i>Difficulty of establishing who is data controller or processor</i> .....	48
<i>Difficulty in determining applicable laws</i> .....	51
<i>Ability to audit</i> .....	51
<i>Problematic reliance on the US Privacy Shield</i> .....	52
<i>Summary of Problem 4</i> .....	53
<i>Recommendation 4: Facilitate and coordinate rights-respecting contracts between schools and EdTech providers</i> .....	54
<b>Conclusions</b> .....	<b>55</b>
<i>Looking ahead</i> .....	56
<b>Annex 1: Data processed by Google Classroom and ClassDojo</b> .....	<b>58</b>
<b>Annex 2: Dutch investigation of Google G Suite (Enterprise) for Education</b> .....	<b>64</b>
<b>Annex 3: Instructions for Schools Administrators on how to customise additional Google services in Google Workspace and their respective terms of service</b> .....	<b>66</b>
<b>References</b> .....	<b>69</b>
<b>Endnotes</b> .....	<b>83</b>

## Foreword

For a decade or more we have understood that a child's online and offline life are intertwined and interconnected. What happens in one environment affects behaviours and outcomes in the other. These effects have been of deep concern to civil society, parents, government and young people themselves. Which makes it at best surprising and at worst sinister that the rise of EdTech in schools has not been greeted with more critical and regulatory attention.

What is happening in our schools is no less impactful on children than in any other environment. Indeed, as this report argues, the processes and practices of EdTech deliberately, seamlessly and permanently extracts children's data for commercial purposes – purposes that may not be aligned with the best interests of the child, the broader education community or indeed the expectations of society more broadly.

As Donald Rumsfeld said, "There are things we know we know. There are known unknowns. And there are also the things we don't know we don't know." The authors of this report can only speak with certainty about what they can see but they are rightly anxious about what they can see they can't see and the things they can't see they can't see! A child's mood at school is fair game for commercial exploitation, parents given non-choices that allow long-term tracking, teachers given responsibility for things they have no control over – or perhaps worse – not given any responsibility for things they have no idea are happening as a result of their engagement with EdTech. And alongside it all, a lack of rigorous accounting for the claimed conveniences or educational benefits – with little or no regulatory or legislative oversight.

This report is one step of a three-year inquiry into education data. As such it offers a riveting glimpse of two services that are chosen primarily for their ubiquity. It is important to establish here that each offers great benefits, and neither is chosen for their poor practice – but rather as an example of a sector norm. The failure lies in the absence of a regulatory framework that ensures education data is fairly taken, benefits children and causes no harm.

Our great thanks are due to the report's authors Louise Hooper, Sonia Livingstone and Kruakae Pothong, to Digital Futures Commissioners on whose wisdom and expertise we depend, to the 5Rights team who make everything happen and to the many teachers, experts and children who have engaged in this work. In the next few weeks, we will publish a series of essays which set out a range of approaches, evidence, arguments and proposals by which educational data could better benefit children. In the months to come the DFC will publish a blueprint for regulation of educational data, our contribution to fixing a problem that is clearly urgent but that, even in an environment that has recently seen no less than nine government data policy initiatives, is simply overlooked.

EdTech is neither good nor bad, and nothing in this report argues that innovation and spread of technology that benefits children and their knowledge or wellbeing should be prevented. Like most things digital, it is simply a question of uses and abuses. As it stands both what we know and what we know we don't know of current practice is not fit for purpose, which means we can only fear the things that we don't know we don't know.

- *Baroness Beeban Kidron OBE*

## Acknowledgements

We thank the many experts we have interviewed during our research, and Ayça Atabey for her help with data protection laws and referencing. We thank the family who walked us through their user experiences with Google Classroom. Thanks also to Baroness Beeban Kidron for her input and guidance, to all our Commissioners at the Digital Futures Commission, and the teams at 5Rights Foundation and BB Partners for their support.

## Executive summary

**There has been an explosion in the use of educational technology (EdTech) in UK schools in recent years to support teaching and the effective day-to-day management of education institutions. While the use of new technologies may offer new opportunities to enhance learning, the expansion of the digital world into educational settings also brings major risks for children’s safety and privacy online. EdTech is increasingly driven by data, much of it personally identifiable data. This means that personal data processed from children during their learning may enter a heavily commercial global data ecosystem, with little known consequences for their immediate or long-term outcomes for children and their prospects in life.**

Heavily funded by government, the speed of adoption by schools increased significantly during the COVID-19 pandemic in response to the need for remote education provision.<sup>1</sup> In 2021, the Department of Education declared that:<sup>2</sup>

---

Schools are expected to use a single, interactive platform such as Microsoft Teams or Google Classroom for their remote education provision.

---

Now, many primary and secondary school children across the country are accustomed to a hybrid learning model, which includes the regular use of numerous online digital classroom tools, such as Google Classroom and Class Dojo. Although fully remote learning ended after the peak of the COVID-19 pandemic, in most schools the use of these digital tools has become a permanent feature, being used during lessons and for homework, among many other uses.

Defining ‘education data’ as personal data collected from children through their participation in school for teaching, learning and assessment, safeguarding and administration, the Digital Futures Commission has established that the implementation and enforcement of law, policy and regulation relating to EdTech has not kept up with the exponential growth of an industry on which UK schools now rely (Day, 2021). We also revealed the difficulties schools face in trying to manage children’s data fairly given the complexity and scale of EdTech companies’ operations (Turner et al., 2022).

**This report examines the vast growth in the volume, range and sensitivity of data collected from children during the school day and across their school years. We conduct two socio-legal-case studies of products widely used in UK schools: one platform (Google Classroom) and one app (ClassDojo). These were selected to illustrate developments in the EdTech sector, since it would be impossible to conduct such an exercise for the hundreds of EdTech companies, large and small, currently used in UK schools.**

We find that both Google Classroom and ClassDojo operate according to opaque privacy policies and legal terms that are inconsistent with data protection laws and that could result in the commercial exploitation of children’s education data.

Last year the Dutch Data Protection Authority proposed banning schools from using Chromebooks and Google Workspace for Education for failing to comply with regulation that would improve transparency and protect children's data and privacy unless Google promptly improved its treatment of children's data, which it did, although Google Search is still banned.<sup>3</sup> This follows an earlier ban in Germany<sup>4</sup> and a more recent ban in Denmark,<sup>5</sup> with further countries considering this too.<sup>6</sup> **The same public scrutiny resulting in improved safeguards is yet to happen in the UK. As a result, British children using Google products at school risk commercial exploitation and data-related risks, as may children having to use other EdTech apps at school.**

This report represents our best efforts at understanding a fast-moving terrain.<sup>7</sup> Its very complexity demonstrates how impossible it is for individual schools, parents and children – even lawyers – to understand how and for what purposes education data are processed from children, let alone to keep up with innovation or to frame effective calls for change.

We find that Google Classroom and ClassDojo have enjoyed a fairly free hand in determining for themselves the parameters for processing children's education data – for example, through their design features, data systems, interpretation of data protection regulation and the wording of their product terms and conditions.

The result is that these EdTech services (similarly to many others) are able to collect unknown quantities and types of personal data from child users during their learning and use this for commercial purposes.

This most commonly occurs through EdTech designs in which the boundary between the privacy-respecting ('core') and the commercial ('additional') parts of the service is made nearly invisible and so it is very easy to cross.

For example, a child may begin their homework within the learning environment required by their school and provided by Google Classroom. But, by clicking on a YouTube link or checking out Google Maps, the child unwittingly loses the data protection provided by Google Classroom, resulting in YouTube or Maps harvesting their personal data, integrating it with other Google-held data to profile them, tracking them, and advertising to them (see our 'experiment with Google Classroom'). The same applies to ClassDojo. ClassDojo also raises concerns for its behavioural profiling and social scoring, and the potential impact of these practices on children's education records and future opportunities.

From the schools' perspective, EdTech tools such as Google Classroom and ClassDojo are both useful and, like many EdTech products, 'free'. However, both case studies reveal how children are actually paying for these services with their data (or by watching advertising), processed through their interaction with additional services such as YouTube, Google Maps or Google Search, accessible within their learning environments. It appears that schools are faced with an ultimatum which means educationally valuable tools can only be used at the expense of children's privacy. We are concerned at the implications that the normalisation of such tools without additional safeguards and checks has for their education, privacy and other rights.<sup>8</sup>

**Through their everyday learning at school, and while using school-provided or recommended services for homework, children are subject to data processing over**



**which they and their school have little or no knowledge or control.** <sup>9</sup> Nominally, schools are the ‘data controllers’ responsible for children’s education and protecting their personal data. But the corporate power of EdTech, its ethos of data maximisation (rather than minimisation), and commercially-motivated policies and designs place a near-impossible burden on any school, parent, caregiver or child wanting to manage how data processed from children are used. The report notes that schools lack the budget, capacity and technical/legal skills required to exercise their responsibilities. This statement is not meant to imply that schools are doing a bad job but that they are placed in an impossible position to navigate the complex technology and regulatory landscapes shaped by plurality of global political, commercial players with competing interests.

Given the growing use of different EdTech products in schools, children’s education data is entering the global data ecosystem where it may be vulnerable to data breaches, further commercial exploitation, and may have long-term consequences for children’s prospects (some that we cannot yet know about but many that we do), given the increasing use of automated processing in the workplace, insurance, universities and other areas. It is likely a person’s academic history, attention span, achievements, failures, strengths and potential for improvements will have all been documented by the time they are 18 years old, and prospective universities or employers may be able to access their “full life and development” files at the click of a button and make decisions based on these files without the person knowing what information influenced that decision or being able to dispute the decision.<sup>10</sup>

**It is highly likely that:**

- **In the course of a typical day, personal data will be collected from children and used for commercial purposes including developing new products, marketing and advertising.**
- **EdTech collects far more personal data than schools or families expect and processes, shares and profits from these data in many ways that they do not know about.**
- **Children lack the knowledge and power to exercise their rights for much of the data collected from them in school, and nor can schools do so on their behalf.**
- **EdTech has a relatively free hand in developing products that prove profitable, shaping the curriculum with little public scrutiny of actual educational benefits and potential harms.**
- **With most education data in corporate hands, other uses of education data that could serve public, community or children’s interests become impractical.**
- **Regulation designed to protect children’s education data, their privacy, and other rights is undermined by EdTech companies’ complexity and lack of public scrutiny about these companies, rendering it less effective.**

Our socio-legal analysis highlights four specific problems with Google Classroom and ClassDojo which we believe are indicative of the wider EdTech sector.

The four problems centre on:

- The near impossibility of discovering how extensive the personal data is that EdTech collects from children,

- EdTech profiting from children's data collected while they learn,
- EdTech's opaque privacy policies and legal terms that do not comply with data protection regulation, and
- The way in which current regulation gives schools the responsibility but not the education, funding nor power to control EdTech's actual data processing of their pupils' personal data.

For each problem, we offer recommendations for government, notably, the Department of Education (DfE), the Information Commissioner's Office (ICO) and, also, for EdTech companies. These are intended to ensure that the commercial interests of EdTech companies do not trump children's best interests, and to relieve schools of an impossible burden of data protection without impeding uses of education data to benefit children and the wider public interest.<sup>11</sup>

The government is keen to develop economic growth in the EdTech sector, already worth £3-4bn to the UK.<sup>12</sup> The global EdTech market was valued at over \$250 billion in 2021, with estimates that this will grow to more than \$600 billion by 2027 (Aritzon, 2021), facilitated by the adoption of hybrid and gamified teaching models, better connectivity, and the introduction of 5G.<sup>13</sup>

However, our analysis raises serious concerns that EdTech used in schools across the country are leaving children vulnerable to commercial exploitation. Without immediate, joined-up action from government, regulators and EdTech companies, children's data and privacy will be put at even greater risk.

Children's learning should never be the subject of opaque profit-driven exercises by powerful tech companies. Parents and teachers must not be put in the position of having to forfeit valuable online learning tools because government and EdTech companies collectively fail to make those spaces safe for children.

Our report is particularly timely since having implemented the UK General Data Protection Regulation,<sup>14</sup> the government now proposes revising its data protection framework.<sup>15</sup> **We recommend that the government should use the Data Reform Bill as an opportunity to consult widely including with civil society and develop clear, accessible and relevant, child rights-respecting regulation. This would lead to a true pro-innovation approach enabling companies operating in the UK to understand and comply with their obligations to children while developing beneficial educational products founded on the principles of the best interests of the child.**

**Problem 1: It is near impossible to discover what data is collected by EdTech**

- Google Workspace for Education’s policies show the multiple types of data collected by the company during children’s use of Google Classroom. Once combined, this is sufficient to construct a full profile of each individual child including their identity, location, biometrics, preferences and abilities. It is near impossible to discover the nature and extent of this data collection.
- ClassDojo primarily processes data input by teachers who observe children’s behaviour when learning in class or doing their homework. These human judgements, which may or may not be fair or biased, are manually entered as facts into the app or website as behavioural (and arguably biometric) data. This may amount to social scoring.
- Biometric data include data processed by sensors that track body temperature, typing speeds, keyboard patterns or patterns of activity within apps, platforms and devices. This type of data appears to be collected in both Google Classroom and ClassDojo. It is unclear how the companies treat such data in terms of processing, data subject rights and regulatory compliance. It is also unclear whether and how this type of data is interpreted or used by other organisations (e.g., by DfE, future schools, universities and future employers) that can access children’s learning records.

**Recommendation 1: Ensure transparency and accountability for processing children’s education data**

- The government should require EdTech providers to state clearly, publicly and transparently the nature of the data they collect from and record about children through their participation in school.
- Biometric data should not be routinely processed in educational settings (Council of Europe, 2020). Bodily and behavioural data should be treated as biometric data and any processing for the purposes of influencing or monitoring a child’s behaviour should accord with the precautionary principle.

**Problem 2: EdTech profits from children’s data while they learn**

- ClassDojo makes it possible for children simply to click on links to outside apps by navigating using links embedded in the ClassDojo app, thereby becoming subject to other privacy policies. While users do not see third-party advertisements, ClassDojo promotes ‘contextually relevant’ information about its own products and those of third parties.
- When a child has access to additional services in Google Classroom, for example because the school has provided links to YouTube or other apps (e.g., Photos, Scholar or Maps) or when the child uses their personal account alongside a school account, or when the parent uses ‘family link’ (for safety purposes), the child is served adverts and their data are collected for advertising purposes.

**Recommendation 2: Ensure commercial interests in education data do not undermine children’s education and best interests**

- The ICO should ensure that, where an EdTech provider operates both a highly protected and a less protected service (as with Google’s core and additional services, or ClassDojo’s school and outside accounts), the different privacy policies should be made very clear to children, parents and caregivers, and schools. This includes at the moment when a child moves from a more to a less protected environment. This might be achieved by design through better signposting during user engagement or school practice through restricting services to only core services (in the case of Google).
- Consideration should be given to developing technical solutions to ensure that safeguards applied to children’s data within the learning environment continue when the child leaves that environment so that children’s education data is not accessible to data brokers or third-party trackers for commercial purposes.
- To ensure commercial interests do not trump a child’s best interests, and to prevent children receiving marketing and advertising messages during their learning, the high privacy-by-default principles of the Age Appropriate Design Code (AADC) should be mandated for all EdTech services. One option would be to require high privacy-by-default for all children’s data obtained from or processed in relation to their education, whichever EdTech services are being used and whether at home or school.
- When using Google Classroom, schools should require children to use a school-created Google account not their personal account, to give the school more control over the core and additional services the child can access.

**Problem 3: EdTech’s privacy policies and/or legal terms do not comply with data protection regulation**

- Both ClassDojo’s and Google Classroom’s privacy policies and legal terms lack transparency and are difficult to follow or use. This is likely to be in breach of the UK GDPR. Google has already been fined for this by the French data protection authority.
- The UK GDPR also requires that data are only processed for the purposes stated by the processor or controller in their privacy policy. According to the Dutch investigations (see Annex 2), the (then) G Suite (Enterprise) for Education does not comply.
- Where consent is the basis for processing, this is unlikely to be valid: (a) in a school setting because of the power imbalance which makes it too difficult for a child (or parent) to refuse consent; and (b) if the data subject does not understand what its consent is given for.
- The 15 standards of the AADC would offer children better protections for their data at school. However, there is confusion about whether the AADC applies to EdTech providers where their service is provided via schools and current practices by said companies do not appear to be compliant.

**Recommendation 3: Ensure that EdTech provides transparent privacy policies and legal terms for their processing of children’s education data in compliance with data protection laws**

- The DfE and devolved education ministries should only permit EdTech providers to operate in schools if they provide fair, transparent and compliant Terms of Service for education data. If the DfE recommends any particular EdTech for use in schools, it should conduct and publish an assessment of the impact of their data processing on children’s education, privacy and other rights, for example via a Data Protection Impact Assessment (DPIA) or Child Rights Impact Assessment (CRIA).
- The ICO should ensure that EdTech providers comply with the UK GDPR and, where applicable, the AADC. It could also recommend to EdTech providers that they comply with the IEEE 2089-2021 Standard for Age Appropriate Digital Services Framework. The DfE or ICO could further decide to warn schools against the use of noncompliant EdTech.
- The DfE, with the support of the ICO, should take urgent steps to ensure for the UK a similar agreement between Google and the Netherlands to limit data processing through Google Classroom and other EdTech as relevant.
- Where consent is relied on as a lawful basis for data processing, DfE should ensure that companies adequately and appropriately seek consent on each occasion it is required from the child or the parent or caregiver, with sanctions for those failing to comply. It is insufficient to rely on any consent given on a one-time basis when an account is created for a child moving between school and home accounts, products or services.
- The ICO should clarify the applicability of the AADC to EdTech based on the actual control over data processing and the technical operation of EdTech procured by schools that qualifies as an Information Society Service (ISS) - i.e. when it requires students to create an account or log in to use the service, or to interact with a service when using a school device, these actions constituting an ‘individual request’ for data to be transmitted via ‘electronic means’ and ‘at a distance’. In our view, the Government should commit to stating that the AADC applies to EdTech even if contracting through schools.
- In addition to compliance with data protection regulation, EdTech providers should base their privacy policies on their DPIA and CRIA, assessing any risks associated with their products and services and the extent of their responsibilities. In doing so, they should consider involving child rights experts and children in developing their products and policies and ensure that the public can understand the implications for child privacy and human rights from the published materials.

**Problem 4: Regulation gives schools the responsibility but not the power to control EdTech data processing**

- The Dutch investigations identified a series of high data protection risks with Google Workspace for Education including lack of purpose limitation, lack of transparency, no legal basis for Google to process the data, and missing or problematic privacy controls. Further, they claim that Google is really the data controller rather than the processor. Google has since made some improvements, but we believe these have not also been implemented in the UK.
- ClassDojo also claims in its contract with schools that the school is the data controller responsible for ClassDojo’s data processing while ClassDojo is the data processor; however, for some aspects of its processing we believe it is in fact the data controller and should be registered with the ICO.
- Both Google and ClassDojo include vague statements in their contracts with schools, creating a difficulty in determining, for example, the applicable laws. Both products provide a right for schools to audit their data processing, but this would be far too costly for any school.
- Both products fail to comply with regulation regarding the transfer of children’s data to the USA: ClassDojo appears not to have updated its Privacy Policy since the EU-US Privacy Shield was invalidated; Google has taken steps which the French data protection authority has ruled ineffective; the Danish government has announced a ban on Google Workspace and Chromebooks in their schools for this reason.

**Recommendation 4: Facilitate and coordinate rights-respecting contracts between schools and EdTech providers**

- The ICO should clarify that the data controller and processor are determined by the actual technical control over data processing as stipulated in the UK GDPR. They should place the burden of proof on EdTech providers in accurately describing their role (both in their contracts with schools and their privacy policies) with regards the personal data collected, be it as data controllers, joint controllers (with schools) or data processor.
- EdTech services operating as data controllers (e.g., ClassDojo) must register themselves on the ICO database of data controllers, and ICO should find a means of ensuring compliance.
- The default settings of any applications offered to a child to use in their learning at school or home must offer high privacy protection, i.e., privacy by default. Where a child can access further digital services through use of a school-approved service, the default high privacy protection should extend to these services. These high privacy settings should preclude children’s education data being processed to target advertisements, for commercial profiling or for developing commercial products and services.
- The ICO should review and update its guidance on overseas data transfers and issue specific guidance to schools. Children’s education data should not be transferred to or stored in a country, such as the USA, that does not offer the same level of protection as the UK GDPR.
- To resolve the ‘David and Goliath’ problem of some 30,000 schools individually tasked with negotiating complex contracts with EdTech companies, government could negotiate with EdTech providers to produce standard contracts, benchmark standards and default settings for schools that comply with data protection regulation and meet educational needs.
- The DfE and devolved ministries should conduct and publish periodic audits of EdTech platforms and other EdTech applications used in UK schools and assess them for compliance with data protection law, regulation and guidance.

## This report

EdTech providers process a broad range of data about children through direct data input (e.g., names, emails, photos, date of birth) by teachers and children as well as that collected during users' interaction with the EdTech services. This occurs via use of management information systems (e.g., SIMS), learning environments (e.g., Google Classroom, Microsoft Teams, ClassDojo Seesaw), school safeguarding systems (e.g., CPOMS) and a host of subject-specific apps (e.g., Oak National Academy, Times Tables Rock Stars, Scratch).<sup>16</sup> Some of this data is classified as sensitive information, partly collected in compliance with statutory reporting obligations (DfE, 2022a).<sup>17</sup>

In combination, and possibly aggregated with other data sources, education data can be processed under 'legitimate business interests' to inform educational content, marking schemes, academic achievements, learning analytics, behavioural profiling, safeguarding and more. It can also be processed for research and to train and improve products among other vaguely defined purposes which undermine the transparency of data practices and user control over data. Users' limited control over the data processed about them highlights the power imbalance between EdTech providers and users which is embedded in the contractual arrangements.

### **This report asks about:**

- **The data processed from children by EdTech companies during their formal education**
- **EdTech providers' data protection and privacy policies and whether these appear to comply with data protection regulations**
- **The likely consequences of EdTech data processing for children's rights, including their privacy and education**

In 2021, Google Classroom was downloaded almost 1.34 million times in the UK, and ClassDojo was downloaded 849,000 times, making them among the most used educational apps (Clark, 2022b).<sup>18</sup> These were chosen as our case studies to illustrate the socio-legal-technical operation of EdTech products and services currently in use in schools across the UK. Accompanying the growth in EdTech is a rising tide of concerns about children's data protection, privacy, protection from commercial exploitation and surveillance, and the technological transformation of the nature of education itself.

Our Digital Futures Commission's EdTech survey found that our case study apps are widely used in UK schools. Children receive little data literacy education. But they value their data privacy and do not wish these apps to share their data with companies.

---

## The Digital Futures Commission's EdTech survey

We asked questions about EdTech to a nationally representative sample of 1014 children aged 7-to 16 years old via Family Kids & Youth's digital wellbeing panel survey in summer 2022. We found that:

- 33% had been asked by their school to use Google Classroom this year (34% primary and 32% secondary pupils)
- 18% had been asked by their school to use ClassDojo this year (27% primary and 9% secondary pupils)
- Only one in 10, or even fewer when it comes to sensitive data, thought it acceptable for the apps they use at school 'to share information about you and your classmates with other companies'
- Less than a third said their school had talked to them about why it uses technology for teaching and learning, and even fewer reported being told about who their education data was shared with, or their data subject rights

---

Our research methods include desk research (see References), a user-journey experiment, and interviews with legal and data protection experts to ensure accurate interpretation of the application of the data protection laws that govern the processing of data from children in schools. Our purpose was not to vilify the two products, nor to compare them for they are very different. Rather, we intend to illustrate the operation of a major platform and a smaller app for what they can tell us about the EdTech sector. Some of the issues we raise are more prominent with Google Classroom (Classroom) than ClassDojo and vice versa; we foreground the prominent case in our analysis and recommendations. Note that the complexities of EdTech and education-related data practices means that the analysis in this report should be taken as indicative rather than definitive. We also acknowledge but have not explored the potential benefits for schools of using Google Classroom and ClassDojo.

The report is structured around our identification of four urgent problems for government, regulator and expert audiences concerned with data protection, education, privacy and child rights. We match the analysis of problems with recommendations and believe that these merit prompt action. For this reason, too, we seek to make this report as clear and accessible as we can, for the problems identified are important to the public.

---

## Definitions

**EdTech:** ‘Education technology (EdTech) refers to the practice of using technology to support teaching and the effective day-to-day management of education institutions. It includes hardware (such as tablets, laptops or other digital devices), and digital resources, software and services that help aid teaching, meet specific needs, and help the daily running of education institutions (such as management information systems, information sharing platforms and communication tools)’ (DfE, 2019, EdTech Strategy).<sup>19</sup>

**Education data:** We use a broad definition of education data, namely personal data collected from children at school and through their participation in school. We distinguish education data processed for purposes of teaching, learning and assessment, for safeguarding and for school administration purposes, also recognising their overlaps.

**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 (ICO, 2021b, p. 9). Cumulatively, personal data in the context of education can include the child’s personal and sensitive data, their identity, biometric data including facial recognition, voice, data relating to their health, interests and use of services, attention span and location data among others (Day, 2021; Persson, 2020). Most of the data collected in EdTech would be considered personal data. Personal data is governed by UK GDPR and DPA 2018 and, under certain circumstances, by the Age Appropriate Design Code (AADC; ICO, 2020).

- **Anonymous data:** is considered the ‘opposite of personal data’ (Purtova, 2018). Companies may use anonymous information which means that the UK GDPR does not apply.<sup>20</sup> Personal data can be anonymised through using anonymisation techniques. However, it is difficult to completely anonymise data (Finck & Pallas, 2020; Narayanan & Shmatikov, 2010; Ohm, 2010). Note that the act of anonymising the data is also a form of personal data processing (Day, 2021), so can only be done on the instructions of the data controller (usually the school).
-

## An introduction to Google Classroom

---

Your all-in-one place for teaching and learning. Our easy to use and secure tool helps educators manage, measure and enrich learning experiences. (Google for Education, 2022b)

---

At school, a teacher can run and manage many aspects of a class from within Google Classroom, either on their desktop or a mobile phone. Marking rubrics can be created, added and reused. Parents and guardians can be given access to Classroom to check on their child's progress. Once students have created a Google account, they can access their assignments, marking schemes, documents, videos and YouTube clips (if enabled by the school) and collaborate across documents or other work environments. A chat function is controlled by the teacher. Advanced versions have more sophisticated technology and currently appear geared towards using machine learning to enable both students and teachers to detect plagiarism and ensure 'originality'.<sup>21</sup> School platform administrators are able to run and view reports to assess both child and teacher engagement, use, security and applications ('apps') usage activity information.<sup>22</sup>

Google Classroom is a 'core service' within Google 'Workspace for Education' that can be used in conjunction with other Google Workspace for Education 'core' services such as Gmail, Docs, Sheets and 'additional' services such as Google Earth, Google Search, Google Maps and YouTube. Google describes Classroom as a 'free blended learning platform' that aims to simplify creating, distributing and grading assignments. Built to streamline the process of sharing files between teachers and students, Google claims it can be used to boost collaboration, streamline assignments and foster communication. Third-party products such as ClassDojo can be integrated with Google Classroom.

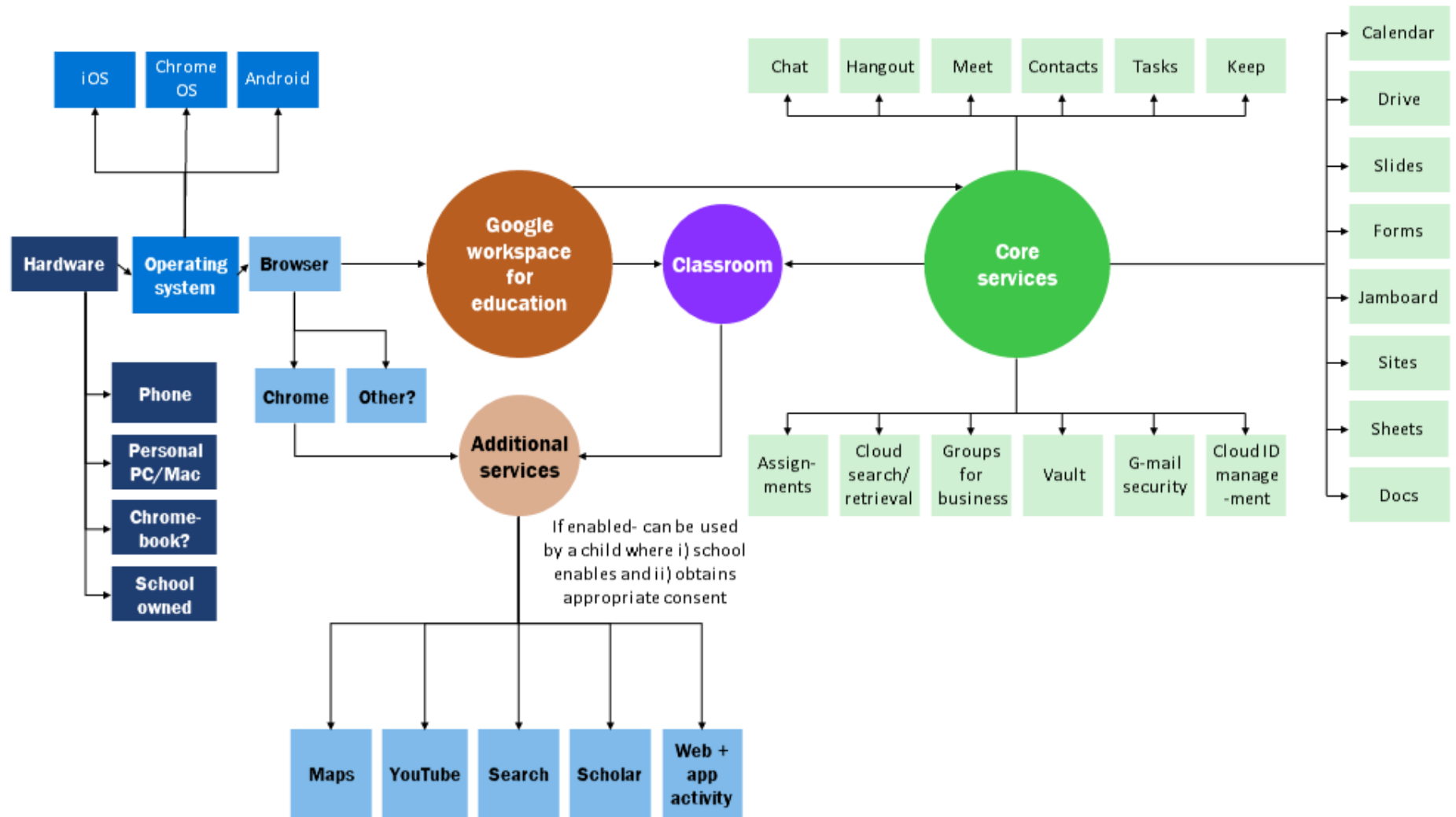
Google Classroom cannot be examined separately from Google Workspace for Education (Figure 1). Google Workspace for Education is both a hybrid teaching/learning and school management system. It is currently offered in four versions, one of which is free. Paid versions have additional security analytics, security features, enhanced educational tools and the ability to make 'originality reports' (Google for Education, 2022a).

Within Google Workspace for Education, core services are provided, and additional services can be enabled by the school. Commonly used services are shown in Figure 2, an image provided by Google. To use Google Classroom each user must create a Google account. Some schools require this to be a school account which gives the school more control over the core and additional services the child can access.

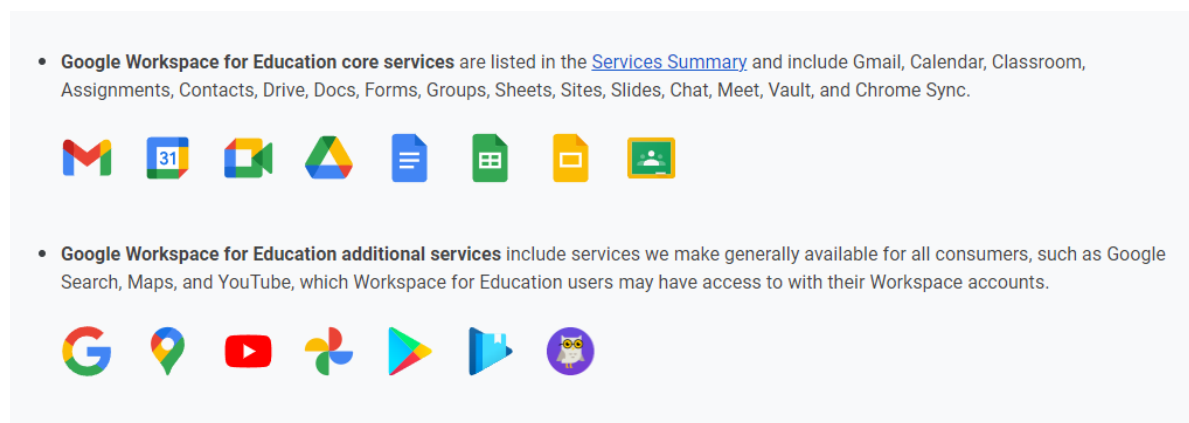
There are fundamental contractual and data processing differences relating to personal data collected under core and additional services, including regarding who is the data processor<sup>23</sup> and data controller<sup>24</sup> and what such data can be used for, including advertising. These are explained below. As also explained below, there is a lack of transparency over the legal terms and privacy policies that apply when additional services are accessed from a core service when using Google Workspace for Education rather than independently e.g., when a child accesses YouTube from within Google Classroom



**Figure 1: Google Workspace for Education**



**Figure 2: Google Workspace for Education ‘core’ and ‘additional’ services (Source: Google)**



## An introduction to ClassDojo

---

ClassDojo connects teachers with students and parents to build amazing classroom communities. (ClassDojo, n.d.-a)

---











ClassDojo is a US-based app offered for free to teachers worldwide to track and nudge children’s behaviour in the classroom. Students sign into ClassDojo using a QR Code, class text code or school-provided Google login. They have their own account where they see their progress and can choose their own avatar. Using ClassDojo Portfolios, students upload their work into a ‘safe space’ – teachers must approve items that students post before they are shared with parents (e.g., through photos and videos of ‘wonderful classroom moments’). Only a child’s parents can see their work, although parents can see the ‘Dojo Points’ (EdSurge, n.d.) given to other children in the class. Teachers decide how work is submitted – take photos, record videos, write journal entries, among other things.

Children are awarded positive behavioural points for behaviours considered by the teacher to be positive and points are deducted for behaviours they consider to be negative (Figure 3). The app is used by teachers to share activities throughout the classroom day, and photos and video recordings of the classroom with parents. Positive behaviours nudged include helping others; keeping on task; participating; persistence; teamwork. Negative behaviours include bullying; disrespect; no homework; off task; talking out of turn; being unprepared.

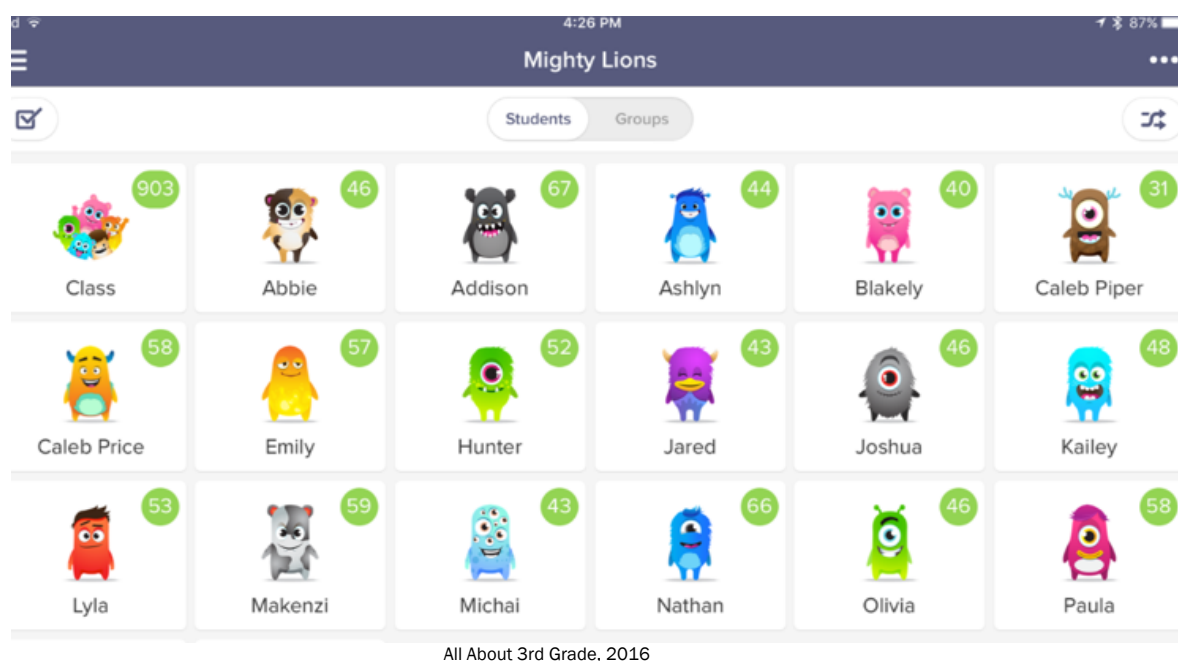
Widely used as an educational platform in the UK, ClassDojo was initially created by venture capitalists ‘to help teachers win back control of crazy classrooms’ (DiGiacomo et al., 2021). As a technology start-up, ClassDojo gained incredible monetary momentum through its noted ability to collect a lot of behavioural data. The Guardian reported in 2018 that ‘the company now appears to be repositioning itself as a social media platform for schools; there is less focus on behavioural monitoring’ (Saner, 2018).

ClassDojo now markets itself as an app to be used alongside Google Classroom to communicate with families and engage students (ClassDojo, n.d.-d). Tools for the teacher include classroom directions app; random group generator; classroom music; classroom noise monitor; think pair share (pairs students and gives them a discussion prompt from the teacher); random student selector; classroom timer; morning meeting app (to share good wishes or instructions for the day).

**Figure 3: ClassDojo point system**

Positive Behaviours		Negative Behaviours	
Behaviour	Points Awarded	Behaviour	Points Awarded
 Enter		 Disruption	
 Cooperation		 Out of chair	
 Participation		 Interrupting	
 Attitude		 Disrespect	
 Exit		 Fighting	

ClassDojo Point System, n.d.



## Problem 1: It is near impossible to discover what data is collected by EdTech

Identifying the education data collected by Google Classroom and ClassDojo would seem the obvious starting point for our analysis. However, this proved difficult. **The legal documents governing Google Classroom and ClassDojo's data processing [see Problem 3] make it near impossible for ordinary users to grasp exactly which data are processed from users and for what purposes. It may even be that the companies themselves do not know and cannot document the full extent or types of education data they process.**

**We first tried to discover what types of data are collected. We map these in Figures 4 and 5 – data collected by Google Workspace for Education and ClassDojo respectively – as discussed in the following sections:**

### Google Classroom

Google's use of different terms to describe types of data as set out below is complex and multi-layered.<sup>25</sup> 'Customer' sometimes seems to refer to the school and at other times to the (child) user. Crucially, the key types of data that might be collected or processed as a result of using Google Classroom are confusingly described using different terms across multiple documents. Quoting from Google's various policies:

- i) Customer Data: 'things you provide or create through core services' (Google Workspace for Education Agreement also known as Google Workspace for Education Terms of Service) ('Education Agreement') (Google for Education, 2021a)) see also:

‘data submitted, stored, sent or received via the Services by Customer or End Users’ (Data Protection Amendment (DPA)) (Google, 2021a)

- ii) Customer Personal Data: ‘personal data contained within the customer data’ (Data Protection Amendment (DPA)) (Google, 2021a)
- iii) Personal Data: for the purposes of the DPA personal data has the same meaning given in the UK GDPR irrespective of whether GDPR applies.<sup>26</sup>
- iv) Service Data: ‘Information we collect as you use core services’ (Education Agreement) (Google for Education, 2021a)
- v) Personal Information: ‘This is information that you provide to us which personally identifies you, such as your name, email address or billing information or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.’ Applies to data collected or processed in Additional Services (Google Workspace (2022) for Education Privacy Notice and Google (2022c) Privacy Policy).
- vi) Information including unique identifiers (Google (2022c) Privacy Policy)
- vii) Non-personally identifiable information: information recorded about users so that it no longer reflects or refers to an individually identifiable user (Google (2022c) Privacy Policy)

Considering previous versions of Google’s education products, Lindh and Nolin (2016, p. 644) concluded that

---

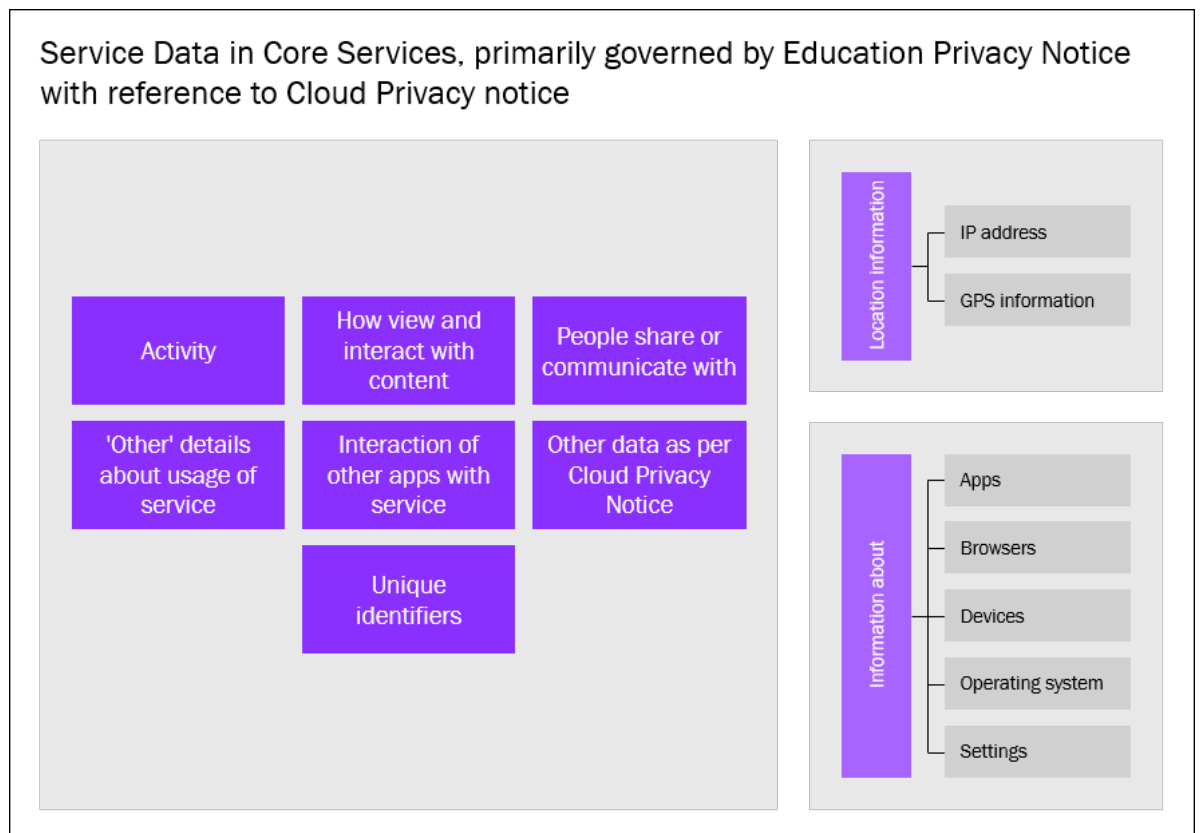
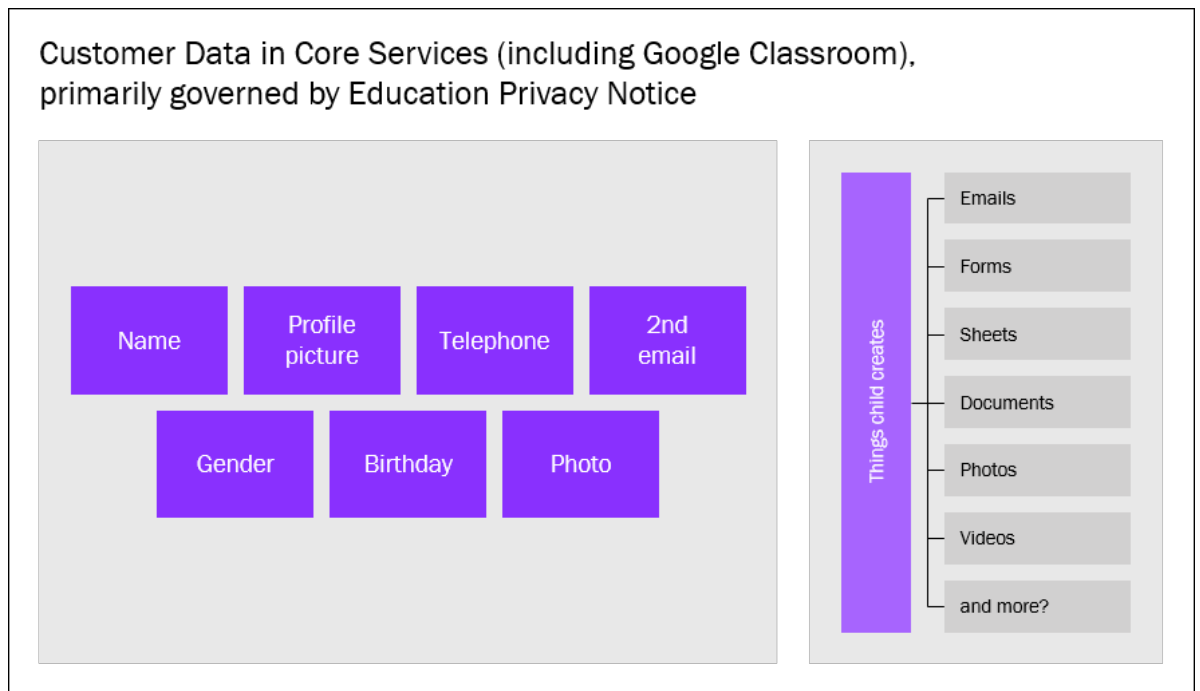
by making an implicit demarcation between the two concepts (your) ‘data’ and (collected) ‘information’ Google can disguise the presence of a business model for online marketing and at the same time simulate the practices and ethics of a free public service institution.

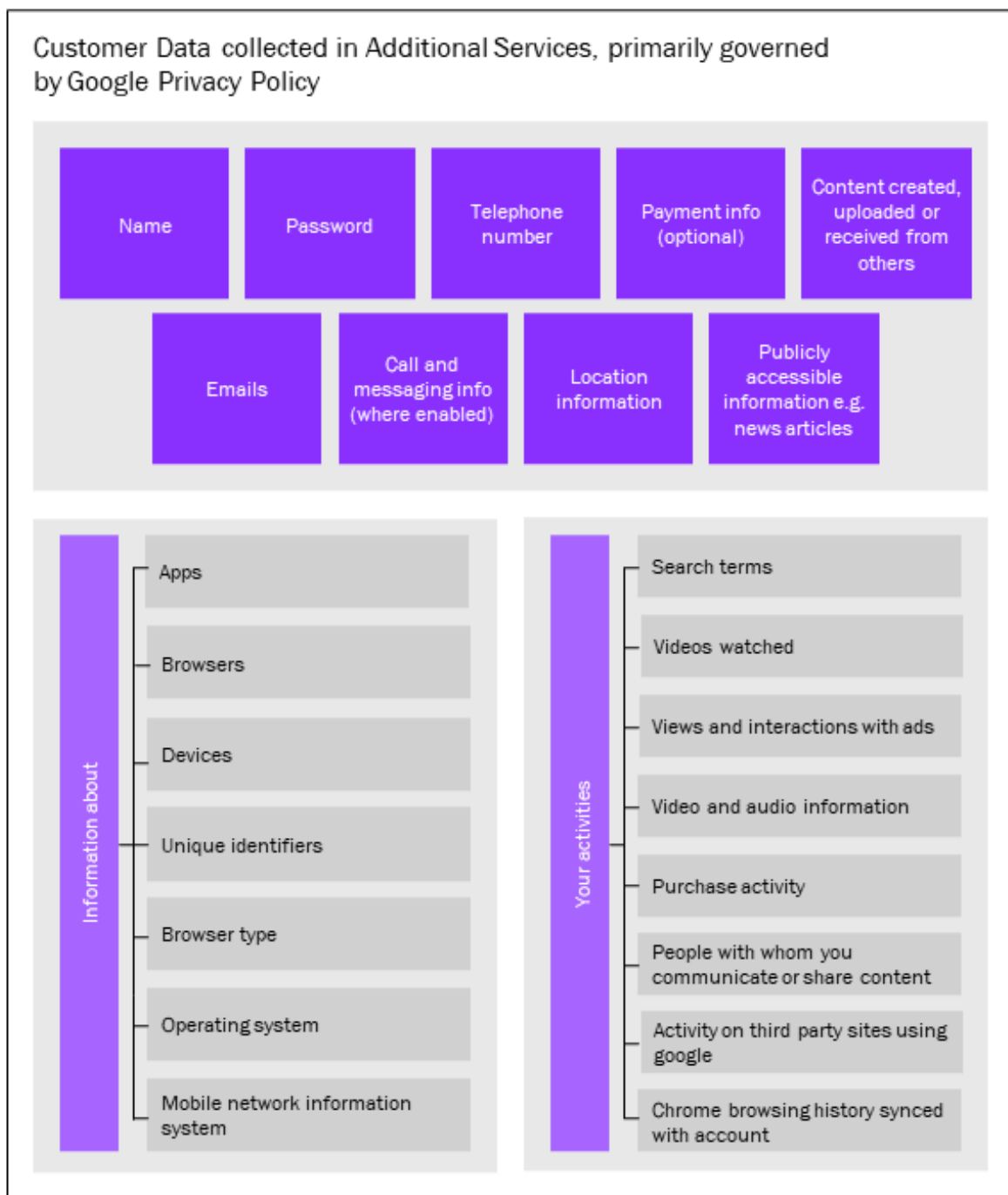
---

Google has unprecedented scale (Statista, 2022) as a company primarily established on a search and advertising business model of extracting and using data from users (Chen et al., 2009, p. 60; Krutka et al., 2021, p. 421). Google has access to significant and detailed data enabling a full profile of an individual child including their identity, location, biometrics, preferences and abilities. It may be impossible, however, for that individual – or the schools and parents/caregivers responsible for them – to comprehend the scope and scale of the data processing relating to them or the implications for their learning, development and future opportunities. This problem applies especially to the processing of sensitive data, metadata and data derived from data aggregation and data analytics.

We map the data collected in Google Workspace for Education products in Figure 4.

**Figure 4: Data collected in Google Workspace for Education products<sup>27</sup>**





## ClassDojo

The descriptions of types of data that may be processed or collected by ClassDojo are:<sup>28</sup>

- (6) 'Personal Data' means any information relating to (i) a Data Subject and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is LEA Data.

(ii) ‘LEA Data’ means what is defined in the Agreement as ‘LEA Data’, ‘Student Data’, ‘User Content’, or ‘Your Data’, provided that such data is electronic data and information submitted by or for LEA (or collected by ClassDojo and Processed on behalf of LEA) to the Services. [‘LEA’ means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed the Int. DPA, Student DPA, and Service Agreement.]<sup>29</sup>

We map the data collected in ClassDojo in Figure 5.<sup>30</sup>

First/last name	App or product username	Password	Age	School address	Local school ID number
Mobile device ID	Photos	Language information	Videos	Behavioral data / feedback	Documents
Drawing	Audio files	IP address	Browser details	Access time	Page views
	Referring URLs	Clicks	Click paths	Active engagement time	

**Figure 5: Data collected by ClassDojo**

A major feature of ClassDojo is the collection of behavioural data that teachers input according to criteria suggested by the app, which can be modified or added to by the individual teacher. Where this data can identify an individual child, it is personal data and is governed by the UK GDPR, DPA 2018 and, in some circumstances, also the AADC. Behavioural data is personal data that is sensitive and may also be biometric data, which attracts higher protections under UK GDPR.<sup>31</sup>

Companies may use different techniques to anonymise personal data. If done successfully, their data processing of the fully anonymised data would not fall under by the UK GDPR, allowing them to benefit from data that they would not otherwise be permitted to use. However, it is difficult to successfully anonymise data (Day, 2021; Finck & Pallas, 2020; Narayanan & Shmatikov, 2010; Ohm, 2010), and the act of anonymising data is also a form of personal data processing, so can only be done on the instructions of the data controller (presumably the school; see later). It is unclear if ClassDojo uses anonymised data from children for product development or marketing and whether schools play a role in enabling this.<sup>32</sup>

Collecting behavioural data entails some degree of surveillance which can be more or less invasive depending on the technology used (Manolev et al., 2019). The behavioural scoring and ‘good’ behaviour attributes encouraged by ClassDojo may result in discrimination against children according to gender, special educational needs or family context. If certain groups score worse than others across the entire school, this could amount to discrimination under Article 14 of the Human Rights Act 1998 or the Equality Act 2010 as it could affect children’s enjoyment of the right to education (Young, 2020).



Constant monitoring of children's behaviour in the classroom and the daily reporting of this back to their parents and other children in the classroom may breach children's right to privacy under Article 8 and freedom of thought under Article 9 of the European Convention on Human Rights as incorporated by the Human Rights Act 1998. ClassDojo even has a feature which allows teachers to publicly share the points scored by children in the class on a class whiteboard.<sup>33</sup>

Some researchers argue that regular updates on student behaviour provided to parents may 'foster parental engagement' (Manolev et al., 2019, p. 43). But for children whose problematic classroom behaviour may be affected by living in homes where they already experience violence, constant behavioural reports may make their lives worse. Whatever the consequences, the behavioural points-based system provided by ClassDojo is a kind of social scoring. In its reports on draft EU legislation on artificial intelligence, the European Economic and Social Committee (EESC) have called for an all-out ban on social scoring in the EU (EESC, 2021; Wilson, 2021).<sup>34</sup>

We note that ClassDojo produces a large amount of anecdotal evidence for the impact of its product, sponsoring teacher endorsements on its website such as one from a teacher claiming that ClassDojo helps children with ADHD to stay on task as a result of continual positive feedback (Connolly, n.d.). Common Sense Media (2020) suggests that ClassDojo's learning management, communication and Social and Emotional Learning (SEL) features 'can promote a wider picture of students' daily experiences and provide transparency for teachers, students and families.' However, although ClassDojo is popular, researchers have found almost no peer-reviewed studies on the app (Krach et al., 2017).<sup>35</sup> Meanwhile, it has been argued that children 'deserve privacy, personal space, and a learning environment where their every transgression is not reported back to their guardians' (Soroko, 2016, p. 70).<sup>36</sup>

## Summary of Problem 1

- **Google Workspace for Education's policies show the multiple types of data collected by the company during children's use of Google Classroom. Once combined, this is sufficient to construct a full profile of each individual child including their identity, location, biometrics, preferences and abilities. It is near impossible to discover the full nature and extent of this data collection.**
- **ClassDojo primarily processes data input by teachers who observe children's behaviour when learning in class or doing their homework. These human judgements, which may or may not be fair or biased, are manually entered as facts into the app or website as behavioural (and arguably biometric) data. This may amount to social scoring.**
- **Biometric data can include data processed by sensors that track body temperature, typing speeds, keyboard patterns or patterns of activity within apps, platforms and devices.<sup>37</sup> Some of this type of data appears to be collected in both Google Classroom and ClassDojo. It is unclear how the companies treat such data in terms of processing, data subject rights and regulatory compliance. It is also unclear whether and how this type of data is interpreted or used by other organisations (e.g., by DfE, future schools, universities and future employers) that can access children's learning records.**

---

## Recommendation 1: Ensure transparency and accountability for processing children's education data

- The Government should require EdTech providers to state clearly, publicly and transparently the full nature and types of the data they collect from and record about children through their participation in school.
  - Biometric data should not be routinely processed in educational settings (Council of Europe, 2020). Behavioural data should be treated as biometric data and any processing for the purposes of influencing or monitoring a child's behaviour should accord with the precautionary principle.
- 

Such vast scope and scale of data processed from children at school raises questions about their compliance with UK GDPR principles of transparency, purpose limitation and data minimisation. We examine these compliance and enforcement issues further in relation to EdTech's unfair terms of service and legal policies (see Problem 3).

But before considering further *how* these EdTech companies fail to comply with data protection regulation, we first looked into why this might be. Commonly if not in all cases, a key purpose is to profit from children's personal data while they learn.

## Problem 2: EdTech profits from children's data while they learn

**Data about children is commercially valuable whether directly input by children, obtained through their engagement with digital technologies for education or leisure, or derived through data aggregation and analytics.** Such data can be used to infer children's preferences and predict their actions in ways useful for advertising, the personalisation of products and services, or product development. This can include informing real-time bidding advertising technology, in-app advertising, contextual advertising, or to encourage product upgrades or additional vendor driven products (Council of Europe, 2020). Such commercial uses of children's data may amount to commercial exploitation (van der Hof et al., 2020).<sup>38</sup>

### Blurring the boundary between core and additional services expands commercial data processing

**Both case studies deploy an EdTech design in which the boundary between the privacy-respecting (core) and the commercial (additional) parts of the service is made nearly invisible and so it is very easy for a child (or school) to cross it unwittingly. In effect, they encourage child users into less private and more commercial environments without highlighting the safety, privacy and rights consequences.** The two case studies deploy different business models which raise different concerns. Put

simply, ClassDojo sells products. Google's advertising-based model centres on the collection and commercialisation of data.

## Google Classroom

The basic, 'user friendly' versions of Google's privacy policies give a clear impression that children's data is not used for advertising purposes at all. Further investigation shows that this is not the whole story. Google's policies say they do not allow adverts in Google Classroom when used in Workspace for Education and that they do not create profiles used to target advertisements in Classroom, noting that advertisements will not be seen while logged into core services using an education account.

**There are two main ways in which advertising enters Classroom and by extension the home environment. Firstly, through establishing 'Google' as a brand of choice for the child and the child being 'educated' in how to use Google and Google-related products and, secondly, by advertising directed at the child while using its additional services.** It also appears that information created by or about children is being collected for other research and development purposes. Indeed, there is evidence that Google combines children's data other data collected from their IP address when using a shared computer at home (Human Rights Watch, 2022).

Where the child uses a version of Classroom provided by the school, using only a school-provided Google account with additional services turned off and Chrome sync disabled, it appears that Google does not process the child's personal data for advertising purposes or developing a profile for advertising. Nor, in these limited circumstances, does it appear that the data are used for Google's own business purposes.

Following the Dutch investigations (see Annex 2) Google agreed, in the Netherlands, to switch the default setting for Ads personalisation to 'off' for new end user Workspace services by Q1 2022 (Nas & Terra, 2021b, p. 12). Where a child has access to additional services, because they are turned 'on' – for example, by a school wishing to use or link to YouTube for teaching purposes or the child uses their personal account alone or alongside a school account, has Chrome sync enabled or uses an Android device (which is a distinct possibility) – they will be served adverts and their data is collected for advertising purposes.

It also appears that Google protects children and students when they use Google Search by automatically signing them out of their school account and treating the data obtained as if it were from an anonymous user so it cannot be used for advertising purposes (Nas & Terra, 2021a, p. 76). We have not been able to see this in practice. But this protection is said not to extend to YouTube, Photos, Scholar or Maps (Nas & Terra, 2021b, p. 4).<sup>39</sup> Other than to promote commercial interests, the reason for this is unclear.

**In short, children are significantly better protected while using core services than additional services. However, the day-to-day experience of school EdTech use is that these two services are closely linked and to some extent merged through pathways that invite teachers and children to additional services without making clear the differences in terms of data processing.** For these additional services, if a school permits a child to use them, significant amounts of personal data will be collected for multiple purposes. YouTube is an example of a popular additional service often used by schools. Privacy is only ensured if the educator embeds the clip of a YouTube video

within Classroom or Slides rather than permitting the child to leave the Google Classroom environment via a browser to view a link to the video (Nas & Terra, 2021b, p. 4), which requires a level of technology literacy that not all teachers possess.

## An experiment with Google Classroom

We undertook an experiment with Google Classroom to see how it was actually used by a nine-year-old child in a primary school in London and a twelve-year-old child during the COVID-19 lockdown. We invited each child and a parent to walk us through how the child and the parent were using Google Classroom as part of the school's remote education. We used the Lightbeam application (a web-browser plug-in) to record the data flow during the child's interaction with Google Classroom to access the teachers' class materials and announcements to students. During this experiment, the parent and the child used FireFox as a web browser to access Google Classroom, and advertising and third-party blockers were temporarily disabled.

According to Figure 6, Google stated that there are 'No ads' in Google Workspace for Education's core service and that 'core service data is not used for advertising purposes' (Google for Education, 2022c). While this statement seems clear, the user interface in Google Classroom is arguably misleading. The interface in Google Classroom does not clearly distinguish between core and additional services. Nor does the interface restrict posting of links to external sites and Google's additional services (e.g., YouTube), which are not governed by Google for Education's privacy policies, nor notify users when they venture out of Google Classroom's ads-free zone.

Figure 6: Google's sales pitch

The screenshot shows the Google for Education website. The main heading is 'DATA SECURITY' with the sub-heading 'Protect your school's data with security built for educational organisations'. Below this are four columns of information:

- Built-in protections:** Safeguard user data with Gmail encryption and identity and access management.
- Strong compliance:** We're committed to transparency and compliance with regulations like the GDPR as well as privacy and security best practices. Learn how you can use Google Workspace for Education services and settings to help meet data protection compliance needs [here](#).
- No ads:** There are no ads in Google Workspace for Education core services, and core service data is not used for advertising purposes. Also in additional services, primary and secondary (K-12) school students' personal information is not used for ads targeting.
- Data transparency:** Schools own their data – it's our responsibility to keep it secure. Google operates our own secure servers and platform services, and we make it easy for admins to manage data security.

At the bottom of the page, there is a cookie notice: 'Google serves cookies to analyse traffic to this site. Information about your use of our site is shared with Google for that purpose.' and two buttons: 'See details' and 'Ok, got it'.

---

The child had unrestricted access to Google's additional services, such as Google Marketplace and Travels when they accessed their school's Google Classroom environment using their home computer and the school-given Gmail account (specifically to sign into Google Classroom).<sup>40</sup>

The child's user journey and Google Classroom interfaces showed no notifications or warnings that the child was stepping out of Google Classroom's high privacy-by-default environment. The child's user journey from Google Classroom into Google Hangout (which is listed under Google Workspace's core service and comes with text chat and video call functions) and their exploration of features and functionalities of Google Hangout revealed that anyone with the child's email address associated with their Google Classroom account could directly invite the child to connect and send not only text messages, but also photos. However, the child was restricted only to receiving images from the third party and text-based (outgoing) communication. These features within Google Workspace's core services could be exploited by criminals and could lead to serious safeguarding problems.

We also found that some teachers share learning materials in the form of web links to video clips hosted by Vimeo and YouTube in Google Classroom's announcement channel called 'Stream' for children to access. Unlike with videos *embedded* within Google Classroom environment, when the child clicked on these video links, they were then taken out of the protected Google Classroom environment and into the third-party tracking zone of Vimeo and YouTube's sites respectively.

According to the data flow captured on Lightbeam, the child's visit to Vimeo and YouTube following a teacher's announcement resulted in cookie surveillance by 92 third-party sites. Figure 7 shows that when the child clicked on the Vimeo link, the child was taken outside the ad-protected environment of Google Classroom and, according to Lightbeam's data capture, the child's interaction with Vimeo's service was tracked by 42 third parties, including 'adservice.google.co.uk', 'analytics.tiktok.com', 'facebook.com', 'amazon-adsystem.com' and others.

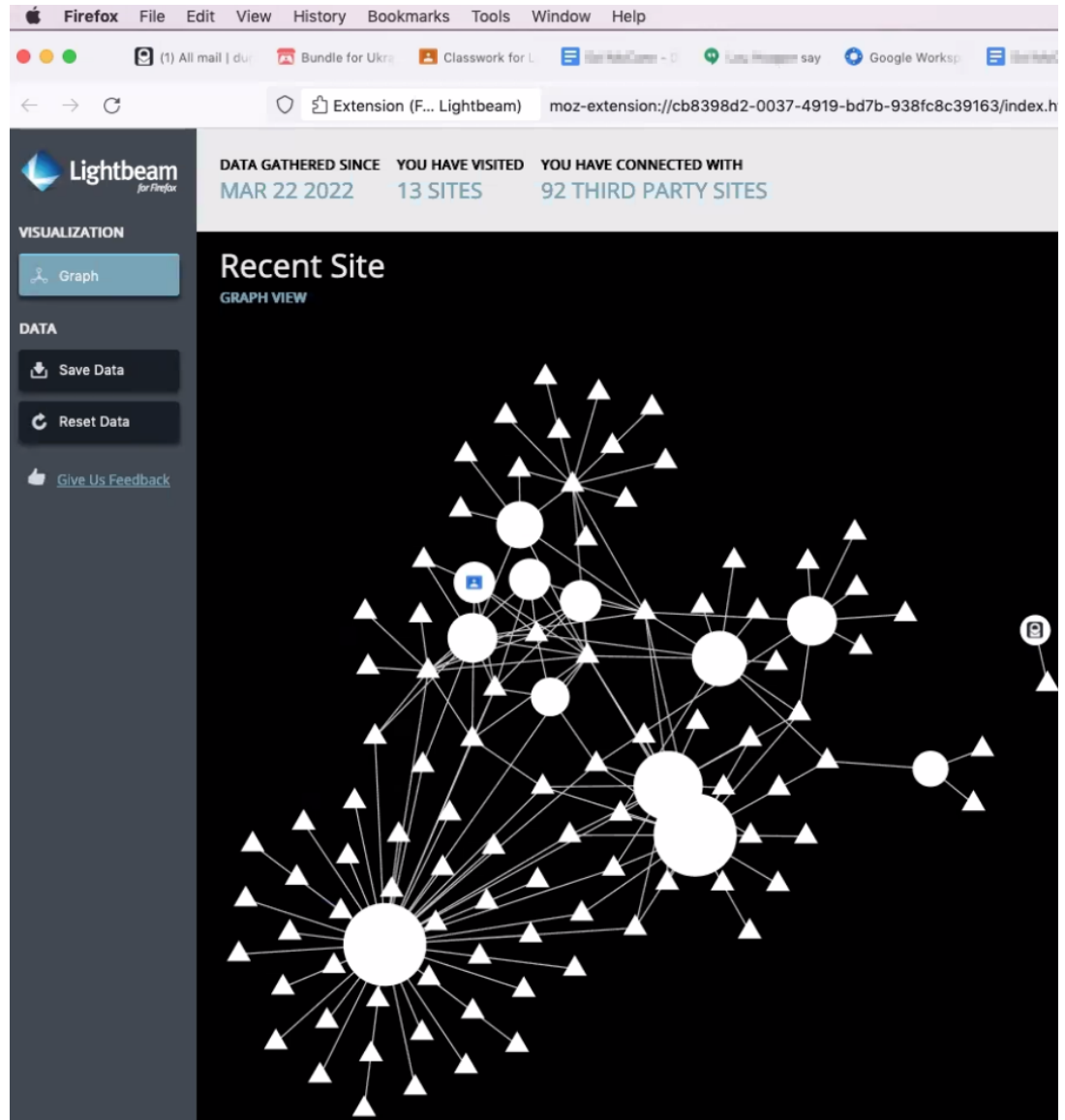
We conducted the same test with a 12-year-old child from a different school, where we found that Google Classroom was more restrictive regarding access to Google's core and additional services: fewer core and additional services were available (visible) to the child. This suggests that schools may take different approaches to setting up Google Classroom, possibly as a result of different levels of awareness or kind of risk/benefit calculation. Google's advertising-driven business model does not appear to aid schools in this respect.

**This experiment reveals that seamless user interface obscures the boundaries between core and additional services, making it very easy for users (children, and also teachers, parents and caregivers) to hop between core and additional services without realising their different privacy and data protection provisions or knowing when they have ventured outside the ad-free zone of Google Classroom.**

These problems could be addressed, for example, through design of user interfaces and access controls, for example, through pop-up notification to remind users that they are about to leave the ads-free zone of Google Classroom and the consequences that such actions entail, or completely blocking access to or departure from Google Classroom to inferior privacy protection sites.

---

Figure 7: Lightbeam visualisation of third-party tracking connected with Google Classroom usage in a primary school in London



JSON	Raw Data	Headers
Save Copy Collapse All Expand All (slow) Filter JSON		
▼ vimeo.com:		
hostname:		"vimeo.com"
▶ favicon:		"data:image/x-icon;base64...AAAAAAAAAAAAAAAAAAAAAAB"
firstPartyHostnames:		false
firstParty:		true
▼ thirdParties:		
0:		"cdn.cookie law.org"
1:		"geolocation.onetrust.com"
2:		"155vod-adaptive.akamaized.net"
3:		"accounts.google.com"
4:		"www.googletagmanager.com"
5:		"app.link"
6:		"api.branch.io"
7:		"www.google.com"
8:		"analytics.tiktok.com"
9:		"websdk.appsflyer.com"
10:		"connect.facebook.net"
11:		"www.googletagservices.com"
12:		"www.google-analytics.com"
13:		"securepubads.g.doubleclick.net"
14:		"googleads.g.doubleclick.net"
15:		"stats.g.doubleclick.net"
16:		"wa.appsflyer.com"
17:		"www.google.co.uk"
18:		"wa.onelink.me"
19:		"www.facebook.com"
20:		"js-agent.newrelic.com"
21:		"fonts.gstatic.com"
22:		"bam-cell.nr-data.net"
23:		"lh3.googleusercontent.com"
24:		"sc-static.net"
25:		"3797665.fl.doubleclick.net"
26:		"bat.bing.com"
27:		"cdn.pdst.fm"
28:		"tr.snapchat.com"
29:		"js.sentry-cdn.com"
30:		"adservice.google.com"
31:		"cdn.taboola.com"
32:		"snap.licdn.com"
33:		"pubads.g.doubleclick.net"
34:		"us-central1-adaptive-growth.cloudfunctions.net"
35:		"browser.sentry-cdn.com"
36:		"i.clarity.ms"
37:		"trc.taboola.com"
38:		"adservice.google.co.uk"
39:		"trc-events.taboola.com"
40:		"px.ads.linkedin.com"
41:		"aax-eu.amazon-adsystem.com"
42:		"s.amazon-adsystem.com"

## ClassDojo

ClassDojo asserts that 'student information' (i.e., children's personal data) is not used for 'behaviourally targeted or third-party advertising' and that information collected from students is never used or disclosed for third-party advertising. When the child is logged in to their school account, they will not see third-party advertisements. But ClassDojo does permit contextually relevant education content for showing either their own products, such as Premium Features, or third-party products and services that ClassDojo believes may be of interest to the student.

**ClassDojo uses 'information' (including children's personal data) collected through the use of its services to improve and develop new products (as does Google, see below).** Its privacy policy states that

---

This policy does not apply to websites or services or practices of companies that ClassDojo doesn't own or control, such as third-party services you might access through links or other features (e.g., social media buttons, email campaigns, push or in-app notifications, or YouTube videos) on the Service. These other services have their own privacy policies, and we encourage you to review them before providing them with personal information. (ClassDojo, 2022a)

---

ClassDojo also invites children to register on ClassDojo through Google Login (ClassDojo, n.d.-c), and children can grant third-party access to Linked Accounts via like and share buttons on social networks such as Facebook and Google/YouTube. Where children register through an authentication service such as those provided by Google, Microsoft or Facebook, ClassDojo also stores and uses certain information already associated with the authentication service (ClassDojo, 2018a).

## Blurring the school/home boundary expands commercial data processing

**When EdTech links home and school, this can result in surveillance of which families are unaware, and data processing that includes biometrics, behavioural data, profiling and tracking. This may generate a data shadow that follows the child into adulthood, embellished with emotions and behaviours 'learned' from the child's past uses of technology and data input by others about them** (Lupton, 2021; Lupton & Williamson, 2017; Nemorin, 2017). The risk is that latent adverse or discriminatory outcome may result from decisions made on the basis of the child's data shadow rather than the child him/herself (Persson, 2020).

When using either Google Workspace for Education and ClassDojo, children or their parents or caregivers are encouraged to set up additional accounts for themselves or the child which may override any privacy protections put in place by the school and cause data from the home environment to leak into the school data ecology.



## Google Workspace for Education

---

Through Google Meet, teachers invite themselves into the homes of each of their students, recreating the power of the school house in each child's home. The teacher's voice, presence and power sit on a child's desk, in a child's lap, and at a child's kitchen table. In demanding cameras on, the teacher asks each student to share their private space with every other student and the teacher. (Gleason & Heath, 2021, p. 33)

---

In its materials for parents and guardians of users of its Education products, Google encourages the creation of a second account for the child so that it can be linked to the school account enabling both to be managed with 'family link'. The stated reason is that this enables the parent or guardian to set parental controls across the accounts.

What is not made clear is that this has the potential to take the child outside protections put in place by the school in the school account, shifting responsibility for data protection to the caregiver (Google, n.d.-c). It may also result in 'home data' (e.g., parents' browsing history) being linked to school data. Defend Young Minds (2021) has published an easy-to-follow set of guidance on how to set up privacy-protecting Family Link parental controls. The instructions are rather long because there are so many steps that need to be taken by parents and caregivers to protect children's privacy.

## ClassDojo

Similar problems may arise with ClassDojo. In the final paragraph of Appendix 3 to the International Addendum (see pp.37-38) it is stated that the contract excludes data from 'Outside School Accounts' which are personal accounts that may be held by students, parents or family users in addition to school accounts. Yet it notes that an Outside School Account may be linked to their student account (ClassDojo, n.d.-g). The contract between the school and ClassDojo does not cover information a student, parent, or family provides to ClassDojo through Outside School Accounts independent of the student's, parent's or family's use of ClassDojo under the direction of the school. The ClassDojo help desk states that linked accounts are only linked by having the same login details, and the data is stored separately. Teachers cannot access the data entered by parents in the Outside School Account.

## Summary of Problem 2

- **ClassDojo makes it possible for children simply to click on links to outside apps by navigating using links embedded in the ClassDojo app, thereby becoming subject to other privacy policies. While users do not see third-party advertisements, ClassDojo promotes 'contextually relevant' information about its own products and those of third parties.**

- **When a child has access to additional services in Google Classroom, for example because the school has provided links to YouTube or other apps (e.g., Photos, Scholar or Maps) or when the child uses their personal account alongside a school account, or when the parent uses ‘family link’ (for safety purposes), the child is served adverts and their data are collected for advertising purposes.**
- 

## Recommendation 2: Ensure commercial interests in education data do not undermine children’s education and best interests

- The ICO should ensure that, where an EdTech provider operates both a highly protected and a less protected service (as with Google’s core and additional services, or ClassDojo’s school and outside accounts), the different privacy policies are made very clear to children, parents and caregivers, and schools. This includes at the moment when a child moves from a more to a less protected environment. This might be achieved by design through better signposting during user engagement or school practice through restricting services to only core services (in the case of Google).<sup>41</sup>
  - Consideration should be given to developing technical solutions to ensure that safeguards applied to children’s data within the learning environment continue when the child leaves that environment so that children’s education data is not accessible to data brokers or third-party trackers for commercial purposes.
  - To ensure commercial interests do not trump a child’s best interests, and to prevent children receiving marketing and advertising messages during their learning, the high privacy-by-default principles of the Age Appropriate Design Code should be mandated for all EdTech services.<sup>42</sup> One option would be to require high privacy-by-default for all children’s data obtained from or processed in relation to their education, whichever EdTech services are being used and whether at home or school.
  - When using Google Classroom, schools should require children to use a school-created Google account not their personal account, to give the school more control over the core and additional services the child can access.
-

## Problem 3: EdTech's privacy policies and/or legal terms do not comply with data protection regulation

**The legal documents governing children's education data processing are complicated and multi-layered for both Google Workspace for Education and ClassDojo. They resemble a complicated jigsaw puzzle for anyone trying to understand them and allow data processing practices to be hidden behind complex legal jargon. Generally, and contra data protection regulation, there is insufficient transparency in the legal documents and processing, insufficient purpose limitation and problems with the lawful basis of processing.**

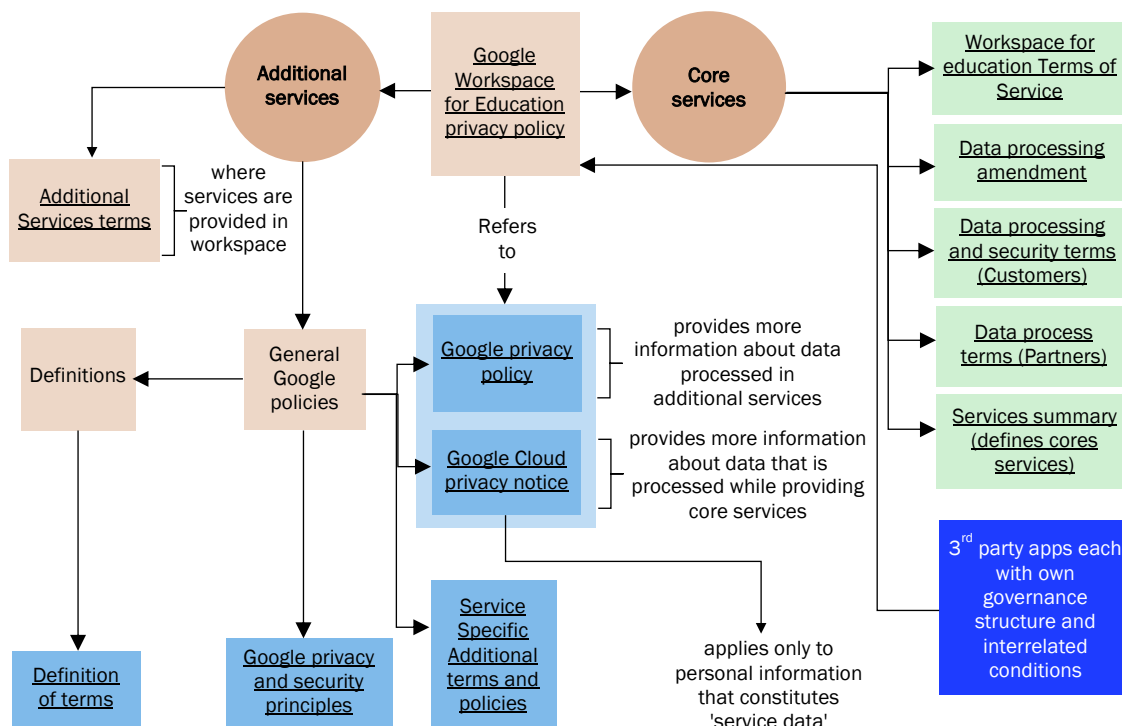
### Google Workspace for Education

Products used in Google Workspace for Education are governed by multiple different privacy policies and Terms of Service. The context in which they are used determines which policy document takes precedence (see Annex 1). For schools to customise their Google Classroom environment and decide what additional services to include, based on careful balance of their relevance and usefulness with their privacy protection, school administrators have to navigate over 60 legal terms (see Annex 3). These diverse and complex legal terms dictate the level of data and privacy protection child users can have, also depending on their context of use. If a legal professional leading the investigation of this case found it challenging to piece together the puzzle of Google Workspace for Education's privacy policies and legal terms, imagine how feasible such assessment is for data protection officers, parents, caregivers and children.

Figure 8 shows our understanding of just some of the main policies and their interrelationship when used by children for educational purposes at school and home. Two points are fundamental to understanding Google's policies:

- i) The difference between Customer data and Service data which are defined by and covered by different privacy policies and terms
- ii) The difference and interrelationships between core and additional services.

**Figure 6: Google Classroom governance structure**



Google Classroom is a ‘core service’ within Google Workspace for Education. Core services are provided for educational use under a school’s Workspace for Education Agreement. The online standard version of this is (confusingly) called the Google Workspace for Education Terms of Service (Google for Education, 2021a) but a school may have offline terms in which case these would govern the use and may not be easily accessible to children, parents or caregivers. Additional terms are provided in the Data Processing Amendment (‘DPA’).<sup>43</sup> The online version of the Workspace for Education Agreement incorporates the DPA at paragraph 5.2.<sup>44</sup>

Core services used within Classroom are then governed by the Google Cloud (2022f) Privacy Notice. This in turn incorporates the Data Processing and Security Terms (Customer) (Google Cloud, 2021).

Google states that the privacy terms for both core and additional services are determined by the Google Workspace for Education Privacy Notice (Google Workspace, 2022). This policy states it is consistent with the Google (2022c) Privacy Policy and the Google Cloud (2022f) Privacy Notice. Where specific commitments differ in those notices and policies the Workspace for Education Privacy notice takes preference, followed by the Cloud Privacy Notice, then the Google Privacy Policy.<sup>45</sup> The example given by Google is:

---

‘For example, the Google Privacy Policy has a description of personalized ads that isn’t relevant to Google Workspace for Education users in primary and secondary schools (K-12), and this notice clarifies that we don’t show personalized ads to those students.’ (Google Workspace, 2022)

---

As noted earlier (Problem 2), although Google emphasises that for users of Google Workspace for Education core services, no ads are shown and no ‘personal information’ collected in core services is used for advertising purposes, ads can still be shown where additional services are used e.g., YouTube.

Additional services are governed by Google [Terms of Service and Privacy Policy](#) (Google, 2022d) and service specific terms (of which there are many) (Google, 2022b). The [Services Summary](#) (Google Workspace, n.d.) sets out and defines the core and additional services. Finally, the Cloud Privacy Notice refers to the [Data Processing Security Terms \(customers\)](#) for Google Cloud services.

---

For teachers and students, the moment users step out of Classroom, the traditional extractive model still applies – that is, even the data collected within the confines of Classroom is still used to refine Google’s tools. They use all the data collected from Google Docs, for example, to train the algorithms for the company’s AI models. Anyone who uses Google Docs is contributing to that process. If a teacher assigned a YouTube video to watch, that extractive model applies.  
(Gulson et al., 2021)

---

To help guide schools, parents and children to understand these complex policies Google has provided further information for schools in its [Privacy & Security Centre](#) (Google for Education, n.d.-b). Tools for families include the ‘Safety Centre’ and a ‘Tech Toolkit for Families and Guardians’ is available on YouTube (Google, n.d.-d; Google for Education, 2020). This includes guides to G Suite for Education (the previous version of Google Workspace for Education), Classroom, Chromebooks and Security. These are easy to understand and accessible but do not really provide full answers to the key questions of what data is collected and what Google does with it.

It is necessary to look carefully at the documents to see which types of data are being referred to and which are excluded when Google explains how the data is used and shared. Even then it is often unclear not only what data is being processed but also which processing purpose or lawful basis applies to which category of data as the policies are drafted so widely.

**Particular difficulties arise if third-party apps are used within Google Classroom. For this, users would have to analyse both Google’s myriad privacy policies and the third-party app’s policies and work out how they interact with each other, which policy takes precedence and how this affects the controller/processor relationship, lawful bases of processing, data storage and transfer clauses among other issues.**

## ClassDojo

The Terms of Service on ClassDojo’s (2018d) website are layered, with the top layer being in non-binding simple language, and the next layer being the lengthier legal fine print. Layering can be a helpful way to assist users to navigate the terms and conditions and is a technique recommended by the ICO (2021c) to help users reach important parts of legal terms. However, where layers also link to external documents within those

layers, the outcome may be the exact opposite creating very complicated and difficult to navigate legal terms.

- i) The Terms of Service (ClassDojo, 2018d) are generally applicable to all users and are to be read in conjunction with different additional terms that apply to each of teachers, students and parents.
- ii) If the school purchases premium features (ClassDojo, n.d.-b), they are subject to an additional set of terms (ClassDojo, 2018c) only applicable to these premium features.
- iii) Schools are also subject to the separate Privacy Policy (ClassDojo, 2022b).
- iv) Schools are subject to a Student Data Protection/Privacy Addendum (ClassDojo, 2021b) which is signed by the school and takes precedence over the Terms of Service where there is any conflict. The Terms of Service and Student Data Protection/Privacy Addendum published on ClassDojo's website refer only to US laws including the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Rule (COPPA) (ClassDojo, 2018d). The Addendum applicable in the UK must be requested by email.

As ClassDojo (2018d) states:

---

These Terms of Service contain general terms that apply to you as a user of the ClassDojo Service ("User"), along with additional terms that may apply to you as a User registered as a teacher, school leader, aide, or other similar personnel ("School Personnel"), or a parent. If you are School Personnel, you will also be subject to our Student Data Protection Addendum ("DPA"). If you are purchasing any premium features like ClassDojo Plus ("Premium Features") through the ClassDojo Service or partake in any sweepstakes, giveaways, or promotions we may offer you will be subject to the ClassDojo Premium Features and Promotions Terms. The DPA and the Premium Features and Promotions Terms (collectively "Terms") are hereby incorporated by reference.

---

On a separate ClassDojo Helpdesk webpage, readers are given an email address to contact if they would like to review or sign their International Student Data Privacy Addendum (International Addendum) (ClassDojo, n.d.-f). We emailed them on 21 December 2021, asking for the agreement that would apply to the UK, and received a response the next day containing links to view the International Data Processing Addendum online (ClassDojo, 2021a). The response time was good, but the requirement to email the company for a copy of this agreement adds yet more admin and delay, which makes it highly unlikely that anyone apart from a school, or a parent with a particular interest in children's data, would ask to see these terms.

**Navigating these multiple policies and agreements is difficult and time consuming and adds a level of complexity that is likely to discourage most users from reading any of the fine print. We estimate that it would take a lawyer with expertise in privacy law a week to read and comprehend the different intersecting policies and**

**potentially months to analyse the extent of the implications for children's rights in a given school, especially as data is transferred to a number of sub-processors and stored in the USA. Of course, it is impossible for individual schools to conduct such thorough review of legal terms and privacy policies for each potential EdTech provider, and these are, in any case, often non-negotiable.**

---

## International challenges to EdTech's use of children's data

Two recent investigations from the Netherlands (see Annex 2), among other European actions, and New Mexico (United States District Court for the District of New Mexico, 2020) resulted in improvements that are also needed in the UK.

- In the Netherlands, a very detailed and technical DPIA conducted by Privacy Company identified multiple high risks of using G Suite for Education (as it then was) (Nas & Terra, 2021a).<sup>46</sup> The Dutch Data Protection Authority was so concerned by these findings that it warned the educational sector on 31 May 2021 to stop using Google Workspace if the high risks could not be mitigated before 21 August 2021, the start of the school year. Similar concerns applied to the use of Chromebooks and the Chrome browser (Nas & Terra, 2021b).
- Negotiations were entered into with Google which averted possible enforcement by the Dutch Data Protection Authority with Google agreeing to take measures to mitigate the risks for both the free and paid-for versions of Workspace for Education with only two substantial differences. Firstly, paying customers can choose to store data for core services in data centres in the EU rather than the USA and secondly, have access to more security features such as device management (Nas & Terra, 2021b). The 'Update DPIA report on Google Workspace for Education' sets out the outcome of those negotiations, provides a list of measures administrators should take to mitigate the remaining risks, and has a section on 'Specific risks and measures for children' (Nas & Terra, 2021b, pp. 31-35). As Hans Biemans, Executive Board of the University of Groningen, who commissioned the DPIA said: '*We've made ourselves bigger toward Google, and you can see that's working*'<sup>47</sup> (SURF, 2021a).

Although Privacy Company identified numerous data protection risks, and although a partial resolution was achieved through negotiation by the Dutch Government and Data Protection Authority with Google,<sup>48</sup> it is not known whether those risks exist for pupils in the UK, whether the amendments obtained by the Dutch are equally applicable to children in UK schools, and whether the changes and improvements agreed to by Google are being monitored by the UK authorities. We doubt that the problems raised are limited to Google products.

---

Similar issues have also arisen in Denmark because it is proving too difficult in practice for schools to implement the necessary settings to ensure compliance with GDPR. The consequence is that children's personal data could be transmitted to third countries in breach of their data rights protections. In July 2022 the Danish authorities issued a ban

on the use of Google products in public schools in Helsingør Municipality,<sup>49</sup> following an earlier ban in Germany.<sup>50</sup> Other countries are considering related actions.<sup>51</sup>

---

**In a second telling case, in February 2020 the Attorney General of New Mexico filed a complaint against Google in the State Court based on allegations of deceptive, pervasive and obscured data collection practices.**

- The complaint concerned the swathes of information collected about children while they used G Suite for Education, notably its additional services (United States District Court for the District of New Mexico, 2020). Ultimately the case was settled by agreement whereby Google agreed among other things to enact a number of reforms including the provision of funding and tools to New Mexico schools, introducing a requirement that apps implement age screening measures to ensure that they do not collect information from children under the age of 13, and increasing parents' knowledge of the information that apps collect from their children (Attorney General of the State of New Mexico, 2021; Gold, 2021).
- One risk-mitigating measure taken by Google as a result of the New Mexico litigation is the introduction of 'Control by Age' (Google, 2022a). From September 2021, this enables administrators to set access controls to some additional 'Google services based on age: YouTube, Google Search, Google Play, Google Maps and Google Earth, Google Photos. Users under 18 are restricted from using other additional services regardless of the Admin console setting.

Privacy, data and/or child rights issues are often resolved by negotiation leading to policy improvements and bespoke contractual or other agreements rather than court judgments that would enable others to rely on them. Hence it is unclear whether settlements and negotiated agreements reached elsewhere will have full effect in the UK, even when they involve prominent companies also operating here and even when UK children would clearly benefit.

---

## Insufficient purpose limitation and lack of lawful basis

**Because of the power imbalance between schools and EdTech companies, resulting in the difficulties identified above, schools as data controllers are not always able to identify, control or limit the purposes for which different types of personal data are processed or, even, to know how data are being processed.**

---

Purpose limitation is the most difficult principle to comply with in big data processing because it [big data processing] is precisely invented to gain new insights by combining data in different way. (Nas & Terra, 2021a, p. 134)

---



Article 5(1)(b) UK GDPR requires that personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the ‘purpose limitation’). Only data controllers can decide the purposes for which data is processed and must be able to show that they are able to comply with this purpose limitation. Data processors, by contrast, cannot determine the purpose of the processing nor whether any further processing is compatible with the original purposes.

## Google Workspace for Education

Google’s policies do not provide an exhaustive list of specific purposes for which data is processed. In respect of core services, Google claims that processing only takes place on the basis of customer (i.e., the school’s) instructions. However, schools have no means of controlling in practice how Google actually processes education data. The Dutch DPIA identified that Google

---

factually processes the personal data in the Customer Data in the Core Services for at least 8, and possibly 20 purposes. These purposes are not specifically and explicitly enumerated as part of the documented instructions of the data controller. (Nas & Terra, 2021a, p. 122)

---

It concluded that the processing of data in the context of (then) G Suite (Enterprise) for Education does not comply with the principle of purpose limitation. This meant that the universities for whom the reports were compiled were unable to identify and therefore rely on any appropriate lawful basis for the processing (Nas & Terra, 2021a, pp. 121-132).

**In additional services, Google is a data controller. The publicly available privacy policy does not sufficiently limit the purposes for which data is used (in addition to the 20 purposes for the core services, an additional 33 have been identified for additional services; Nas & Terra, 2021a, p.83-) and, as we have shown, schools, parents, caregivers or children are unlikely to understand what they are agreeing to.**

In the Netherlands, Google agreed in February 2021 to become a data processor and additionally agreed explicitly to limit processing to three authorised purposes and only where necessary (Nas & Terra, 2021b, p. 14):

- To provide, maintain and improve the Services and Technical Support Services subscribed to by Customer.
- To identify, address and fix security threats, risks, bugs and other anomalies.
- To develop, deliver and install updates to the Services subscribed to by Customer (including new functionality related to the Services subscribed to by Customer).

We have found nothing on whether Google has now implemented this also in the UK.

## Consent as a basis for processing educational data

**Requiring consent as a basis for processing education data is highly problematic (Barassi, 2020). This is because, in education contexts, there is a power imbalance which means the consent is unlikely to be valid.** This is because:

- It is often the parent or educator, rather than the child, who is asked to give consent.
- Consent from the child, when sought, is often by way of a tick box without the child understanding what they are consenting to.
- Adults or children asked for consent are expected to read lengthy terms of service and other policy documents that seem to be written by lawyers to potentially obfuscate the company's intentions (see Krutka et al. (2021); Lindh and Nolin (2016); United States District Court for the District of New Mexico (2020)).
- It can be very difficult for a parent or child to refuse consent for fear of damaging the child's education or ostracising them from their peers.<sup>52</sup>

## Google Workspace for Education

Google relies on consent as the lawful basis of processing and requires the school to obtain consent from a parent or guardian for the use of additional services (Google for Education, 2021a , para 3.5). Two problems arise:

1. Consent should only be used as the basis for processing children's data in an educational setting when none of the legal bases under Article 6 UK GDPR apply (Forbes Solicitors, 2019). This is because consent must be freely given, which is unrealistic for children (or parents/caregivers) in an educational setting where they have little alternative but to use the EdTech product.<sup>53</sup>
2. According to the Privacy Company DPIA, Google stated that if an administrator does not restrict the use of additional services, end users are not asked for (separate) consent when these are accessed (Nas & Terra, 2021a, p. 37; 2021b, p. 14). Instead, it appears that Google will presume that they have consented to the different terms of service for additional services when the user creates the Google account or linked account that they need to access Workspace for Education. It is extremely unlikely a child or their parent will read the raft of terms of service and privacy policies we have identified above (Barassi, 2020, ch 4). As identified above, **consent must be:**
  - a. freely given,
  - b. specific,
  - c. informed and
  - d. unambiguous.

---

Where information is not provided in a concise, transparent, intelligible and accessible form it is unlikely that a valid consent has been obtained (EDPB, 2019).

---

## ClassDojo

Children can have Student Accounts or Outside School Accounts with ClassDojo. The Student Account can be created by the child's teacher, but "only after the teacher represents to ClassDojo that they have obtained the necessary parental consent." The Outside School Account can be created at home after ClassDojo has obtained parental consent directly.

**There is a web page that explains how parental consent is obtained and what it is used for in plain English (ClassDojo, n.d.-e). However, this page refers only to US law (Children's Online Privacy Protection Rule (COPPA)) and we could not find any accessible explanation for UK parents with reference to UK GDPR or other relevant laws**

---

## Lack of transparency: A consequence of convoluted privacy policies and/or legal terms

The lack of transparency over data processing means that EdTech companies are likely to be in breach of Articles 5, 12, 13 and 14 of the UK GDPR and the right of the individual to be informed. A lack of transparency is also likely to result in a lack of lawful basis for processing<sup>54</sup> where consent is relied on (such as in additional services) because consent must be freely given, specific, informed and unambiguous.

In a decision of the French National Data Protection Commission (CNIL) of 21 January 2019 a financial penalty was imposed against Google LLC for lack of transparency, inadequate information and lack of valid consent regarding (in that case) ads personalisation (CNIL, 2019; EDPB, 2019). The decision was based in part on the fact that essential information, such as the data processing purposes, data storage periods or categories of personal data used for ads personalisation were excessively disseminated across several documents with buttons and links on which it is required to click to access complementary information.

Further, the CNIL judged users were not able to fully understand the extent of the processing operations carried out and it was recognised that the processing operations are particularly massive and intrusive because of the number of services offered, the amount and nature of the data processed and combined. The purposes of processing were viewed as being described in too generic and vague a manner, as were the categories of data processed for various purposes. The information was not clear enough for a user to understand that the lawful basis of processing operations for ads personalisation is consent and not the legitimate interest of the company.

---

---

We followed up with the CNIL and were told the case was resolved; they have not reopened any procedure, having established that Google had made the processing of personalised advertising more transparent and its terms more “privacy friendly”.

However, we remark that when using Google Workspace for Education, there are multiple policies with links that must be clicked to build a picture of what data is collected, how it is processed, who is controller or processor, how that relationship changes as a child moves from one product to another and what the lawful basis of processing is at each stage of that process, as shown above and in the detailed tables in the Annex 1.

---

## Problematic application of the Age Appropriate Design Code to EdTech

When the Digital Futures Commission began its work on children’s education data, we had thought that the AADC (or Children’s Code) introduced by the ICO (2020) as a statutory code of practice required by the DPA 2018, would apply to all EdTech. That would have meant that its 15 standards would protect children in their interaction with digital products and services at school as well as at home.<sup>55</sup>

However, it remains unclear and contested under which circumstances the AADC applies to EdTech. ICO (2021a) guidance to EdTech companies is somewhat contradictory, stating generally that ‘The Children’s code does not apply to schools’ and, more specifically, that it does *not* apply where these three criteria are met:

- ‘The edtech service is provided to children via an intermediary such as a school
- ‘The service only processes children’s data to fulfil the school’s public tasks and educational functions
- And ‘The edtech provider acts solely on the instruction of the school, and does not process children’s data in any other form beyond these instructions’.

The same FAQs gives three instances of where the code is likely to apply to EdTech:

- ‘schools procuring “off-the-shelf”, pre-defined, edtech products,
- ‘edtech providers processing children’s data for product development or research – where the research is not the core service procured by a school,
- ‘edtech providers processing children’s data marketing and advertising, or their own commercial purposes.’

Since they do not define ‘off-the-shelf’, ‘pre-defined’, etc., there appears ample leeway for EdTech providers to judge their products out of scope.




---

### The AADC sets out 15 standards of age appropriate design for ‘information society services (ISS) likely to be accessed by children’

1. Make **children’s best interests** the primary consideration in your design and development of digital products and services.
-

2. Conduct a DPIA to assess and manage the impact of your digital products and services likely accessed by children on children’s rights and freedoms.
3. Apply a **risk-based approach** to recognise the requirements associated with age of users and apply the code standards accordingly.
4. Provide **privacy information** in accessible and age-appropriate manners.
5. *Do not* engage in **detrimental use of data** processed from children.
6. Abide by your own **published terms of use and policies**.
7. Ensure high privacy for your products’ and services’ **default settings**.
8. Ensure **data minimisation**.
9. *Do not* **share data** processed from children without a compelling reason.
10. Turn **geolocation options** off by default and notify users when geolocation is active.
11. Provide age-appropriate information and notification to children if and when **parental controls** are in use.
12. Turn **profiling** features off by default in the absence of compelling reasons and protection measures.
13. Do not use **nudge techniques** to manipulate children into providing unnecessary data or weakening their privacy protections.
14. Ensure that your **connected toys and devices** comply with this code.
15. Provide **online tools** to support children to exercise their data subject rights and troubleshoot concerns.

**Figure 9: When does the AADC apply to EdTech**

	<p>AADC Does not apply to schools (though its principles are still relevant).</p>	<p><b>Example</b> School Management Information System.</p>
	<p>AADC Does apply to EdTech services if accessed by children on a direct to consumer basis (e.g., where the child or parent buys an app).</p>	<p><b>Example</b> A parent or child downloads an app from the App Store to help the child learn French.</p>
	<p>AADC May apply to EdTech services where provided through a school and the EdTech provider influences the nature and purpose of children’s data processing.</p>	<p><b>Example</b> A school enters into a contract with Google Classroom or ClassDojo and delivers education to children through these services.</p>

The AADC clearly applies to children's use of social media, games and a host of other digital products and services including EdTech when children sign in and directly interact with these services. Irrespective of where children use these services, as long as children are actually using the services, the AADC requires the default settings of these products to provide a high level of privacy protection and data minimisation and turn off commercial profiling and geolocation by default.

Since children also log in to use and directly interact with EdTech products and services at school and schools often cannot know or control the processing of children's data (see the Dutch DPIA above) it appears that the AADC should apply there too (Figure 9). This means that the collection of IP address and GPS information in Google Classroom's core services and ClassDojo's behavioural-based features must be off by default. It remains unclear whether it is accepted that a child logging into an EdTech product at school is covered by the AADC and we believe they should be.

**However, our case studies revealed that not all standards of the AADC are complied with. For example, ClassDojo could be viewed as profiling children. Google does not provide sufficiently transparent information when a child changes the default settings. As our report has amply documented, privacy information regarding both apps is far from age-appropriate. Ironically, when children move from core to additional services, their data appears even more likely to be shared for commercial purposes.**

### Summary of Problem 3

- **Both ClassDojo's and Google Classroom's privacy policies and legal terms lack transparency and are difficult to follow and understand. This is likely to be in breach of the UK GDPR. Google has already been fined for this by the French data protection authority (CNIL, 2019; EDPB, 2019).**
- **The UK GDPR also requires that personal data are only processed for the purposes stated by the processor or controller in their privacy policy. According to the Dutch investigations, the (then) G Suite (Enterprise) for Education did not comply.**
- **Where consent is the basis for processing, this is unlikely to be valid:**
  - **in a school setting because of the power imbalance which makes it too difficult for a child (or parent) to refuse consent; and**
  - **If the data subject does not understand what its consent is given for.**
- **For ClassDojo, the only available information about parental consent refers to US not UK law. For Google, the information provided is so lengthy that any consent given is unlikely to be informed.**
- **The 15 standards of the Age Appropriate Design Code would offer children better protections for their personal data processed via school. However, there is confusion about whether the AADC applies to EdTech providers where their service is provided via schools and current practices by said companies do not appear to be compliant.**

---

### **Recommendation 3: Ensure that EdTech provides transparent privacy policies and legal terms for their processing of children’s education data in compliance with data protection laws**

- The DfE and devolved education ministries should only permit EdTech providers to operate in schools if they provide fair, transparent and compliant privacy policies and legal terms for education data. If the DfE recommends any particular EdTech for use in schools, it should conduct and publish an assessment of the impact of their data processing on children’s education, privacy and other rights, for example via a DPIA or CRIA.<sup>56</sup>
  - The ICO should ensure that EdTech providers comply with the UK GDPR and, where applicable, the AADC. It could also recommend to EdTech providers that they comply with the IEEE 2089-2021 Standard for Age Appropriate Digital Services Framework.<sup>57</sup> The DfE or ICO could further decide to warn schools against the use of Ed Tech noncompliant with these UK privacy regulation and code.
  - The DfE, with the support of the ICO, should take urgent steps to ensure for the UK a similar agreement between Google and the Netherlands to limit data processing through Google Classroom and other EdTech as relevant.
  - Where consent is relied on as a lawful basis for data processing, DfE should ensure that companies adequately and appropriately seek consent on each occasion it is required from the child or the parent or caregiver, with sanctions for those failing to comply. It is insufficient to rely on any consent given on a one-time basis when an account is created for a child moving between school and home accounts, products or services.
  - The ICO should clarify the applicability of the AADC to EdTech based on the actual control over data processing and the technical operation of EdTech procured by schools that qualifies as an ISS (i.e., when it requires students to create an account or log in to use the service, or to interact with a service when using a school device, these actions constituting an ‘individual request’ for data to be transmitted via ‘electronic means’ and ‘at a distance’). In our view, the Government should commit to stating that the AADC applies to EdTech even if contracting through schools.
  - In addition to compliance with data protection regulation, EdTech providers should base their privacy policies on their DPIA and CRIA, assessing any risks associated with their products and services and the extent of their responsibilities. In doing so, they should consider involving child rights experts and children in developing their products and policies and ensure that the public can understand the implications for child privacy and human rights from the published materials.
-

## Problem 4: Regulation gives schools the responsibility but not the power to control EdTech data processing

Since schools, parents, caregivers and children and even the companies' engineers themselves (Smith, 2020) struggle to understand what data is being collected and how it is used, how can they know whether legislation is being complied with or the implications for child privacy, digital and human rights (Stoilova et al., 2020)? Insofar as it is possible to use EdTech products in ways that ensure good privacy protection, it is not obvious to educators (or children, parents and caregivers) how to do so and nor have they the power to act in children's best interests (Turner et al., 2022).

**While current regulation holds schools responsible for children's education data, EdTech companies undermine schools' control over education data processing, along with children's and parents' ability to object to data processing or manage children's data.**

### Difficulty of establishing who is data controller or processor

**Under UK GDPR, it is necessary to define who is the controller or a joint controller and who is the processor of data (Day, 2021). Deciding which entity is the controller and which is the processor is a question of fact (EDPB, 2021a),<sup>58</sup> regardless of what is written in any contract (EDPB, 2020). According to our understanding, we believe that both Google Workspace for Education and ClassDojo's contracts for use in the UK get this wrong.**

This matters because the controller is responsible for defining the purposes and use of data processing, whereas the processor should only act on the instructions of the controller. The controller therefore has much more responsibility and accountability under UK data protection laws. Data processors also have responsibilities under the UK GDPR but are less likely to be sued for a breach of data protection laws if they have complied with the controller's instructions. Even if both controllers and processors are parties to a lawsuit the largest fine would likely go to the controller, which is presumably one of the reasons why companies appear keen to define themselves as processors rather than controllers.

### Google Workspace for Education

For Customer Personal Data, according to Google's (2021a) Data Processing Amendment (DPA) to Google Workspace:

- i) European Data Protection Law applies to the processing of '*Customer Personal Data*' where the processing is carried out in the context of the activities of an establishment of a customer in the UK or where the data subject is in the UK and the processing relates to offering them goods or services in the UK or the monitoring of their behaviour in the UK (Para 4); and



- ii) Processor and Controller Responsibilities are assigned so that within Workspace for Education core services, including Classroom, Google is the Processor and the Customer is a Controller or Processor as applicable.
- iii) In additional services, Google acts as a data controller and collects a raft of data which it is then able to use for a very wide range of stated purposes (Google Workspace, 2022).

In effect, Google contracts with the school to only use Customer Data to provide the core services and technical support. Service Data is governed by the Google Cloud (2022f) Privacy Notice which states that the controller responsible for Service Data is Google Cloud EMEA<sup>59</sup> unless an agreement has been entered into with a third party who then becomes the controller. However, there is an identified likely difference between the contract and the practice, as explained below.

**The highly technical analysis of core services by Privacy Company<sup>60</sup> concluded that, because of the interaction of Google Products, 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.**<sup>61</sup> Some of that data may be personal data of a sensitive nature or coming within ‘special categories’ of personal data revealing protected characteristics (Nas & Terra, 2021a, p. 64). In the context of Google products 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 initially accepted by Google, through negotiations in the Netherlands, in relation to Dutch schools and universities Google has agreed to become a data processor for this data for three specific purposes rather than the multiple general purposes set out in the Google Cloud Privacy Notice (Nas & Terra, 2021b). This solves some of the high data protection risks identified in their DPIA of lack of a lawful basis where Google and the universities were factually acting as joint controllers (irrespective of what was contained in the DPA). Google has stated that this requires a technical redesign.

Although negotiations between Google and the Netherlands appear to have reached a successful conclusion by the end of May 2022 (Speed, 2022) and some general improvements made, it is unclear whether the measures put in place in the Netherlands have also been put in place in the UK such that the high risks identified in the original report have been mitigated in whole or part for UK schools (Nas & Terra, 2021b, pp. 10-11). **Unless for some reason, the measures agreed with the Dutch are not applicable to UK schools, it is likely that there is no lawful basis for processing children’s data obtained through use of Google Workspace for Education as required in Article 6 UK GDPR owing to the lack of transparency and insufficient purpose limitation.**<sup>62</sup>

## ClassDojo

It is likely that ClassDojo is the data processor under the UK GDPR *for their core services*, and the school is the data controller directing ClassDojo to process children’s data under the legal basis of public task. It is also likely that ClassDojo is either an independent controller or a joint controller for *other aspects of data processing*, regardless of what it says in the contract. In the only UK school DPIA we could find

published online for ClassDojo, the school identified ClassDojo only as a data processor and the school as data controller (Revolution Professional, 2019).

ClassDojo's website details the legal bases under which their app processes children's data and most of these are legitimate interests or contract (ClassDojo, 2018b). Given that ClassDojo defines the purposes and means of data processing in these cases, and that neither of these legal bases are available to schools, it follows that ClassDojo must be the data controller for these kinds of data processing.<sup>63</sup>

**In short, ClassDojo should be defined as a data controller at least some of the time under UK law but ClassDojo seems to get this wrong. However, ClassDojo asks schools to sign a contract which states that the school is the data controller and ClassDojo the data processor, with any further companies who ClassDojo may share data with being defined as sub-processors, which means they still come under the responsibility of the school as the controller.**<sup>64</sup>

This makes the school liable for everything that ClassDojo and its affiliates do with children's education data. This liability also extends to data transferred by ClassDojo to the USA (see below). Schedule 3 to the contract includes standard contractual clauses related to the transfer of children's education data outside of the UK, and states that children's data is stored in the USA. The contract defines the 'data exporter' as '*the controller who transfers the personal data*' and the entity receiving the data as the 'data importer'. In this instance the school has already been defined as the controller, which means they must also be the data exporter.

The school as data exporter is required to agree and guarantee

---

that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State. (ClassDojo, 2021a, Clause 4)

---

The obligations of the school as data exporter include overall responsibility for instructing ClassDojo as the data controller only to process data in accordance with applicable data protection law; ensuring that ClassDojo has sufficient guarantees in place to respect defined technical and organisational security measures and ensuring compliance by ClassDojo with these measures; and fulfilling the legal rights of child data subjects. By contrast, under Clause 5, ClassDojo as the data importer is merely required to comply with the school's instructions and to notify the school if they become aware of legislation that prevents it from fulfilling those instructions (ClassDojo, 2021a).

The section of the contract which specifically addresses liability provides that any data subject (i.e., child whose data is processed by ClassDojo) who has suffered damage as a result of any breach of the obligations set out in the contract is entitled to receive compensation from the data exporter (i.e., the school) for the damage suffered. The child can only pursue ClassDojo for damages if the school '*has factually disappeared or ceased to exist in law or has become insolvent*' (ClassDojo, 2021a, Clause 6).

**ClassDojo is not registered as a data controller in the ICO database which is likely to be in breach of Provision 2 of the Data Protection (Charges and Information)**

**Regulations 2018**<sup>65</sup> pursuant to the **DPA 2018**. This is most likely because it does not consider itself a data controller although, as set out above, we believe this to be mistaken. Since ClassDojo markets its Outside School Accounts to the UK market, for this reason too it has a legal duty to register as a data controller with the ICO.

## Difficulty in determining applicable laws

### ClassDojo

Since, as explained above, the ClassDojo contract for school accounts states that the school is the data controller, this means that the school is responsible for ensuring that the data processing by ClassDojo complies with the requirements of ‘all applicable data protection laws and regulations’.<sup>66</sup> However, the contract does not set out which specific laws ClassDojo considers apply to this agreement or how they apply. This is a startlingly vague and broad statement for schools to agree to. When does ClassDojo consider UK laws apply, and which ones, and when do they consider US laws apply, and which ones? What if there is a conflict of laws?

### Google Workspace for Education

For users of Workspace in the UK, European Data Protection Law is applied to the processing of customer personal data which would include a child’s data. As with ClassDojo, however, the parties ‘also acknowledge that non-European data protection law may also apply to the processing of Customer Personal Data’ (Google, 2021a) although it is not stated explicitly by which laws or when. Again, so broad a statement is difficult for schools to agree to without specific information.

## Ability to audit

**Both Google and ClassDojo provide a right for schools to audit their data processing, but in reality, this would be far too costly for any school to contemplate.**

### Google Workspace for Education

Google’s DPA sets out a range of audit rights for the customer or an independent auditor and includes a discretionary charge (Google Cloud, 2022). Copies of third-party audits are available in the admin console of Workspace.<sup>67</sup>

### ClassDojo

The contract notes that schools have a right to audit ClassDojo to ensure they are complying with the terms of the agreement.<sup>68</sup> However, if they wish to carry out an on-site audit the school must reimburse ClassDojo for their costs incurred, requiring an on-site trip by professional auditors to the US to carry out a complex audit of ClassDojo’s

data processing, to ensure that it complies with both US and UK laws, and on top of that to fund ClassDojo's related expenses.

## Problematic reliance on the US Privacy Shield

Currently, there are unresolved problems raised by the Court of Justice of the European Union (2020) in *Schrems II* which invalidated the EU-US Privacy Shield.<sup>69</sup> Yet at present both Google Workspace for Education and ClassDojo transfer children's data to the USA.

The new Trans-Atlantic Data Privacy Framework to replace the defunct US Privacy Shield framework 'signals intelligence collection may be undertaken only where necessary to advance legitimate national security objectives, and must not disproportionately impact the protection of individual privacy and civil liberties' (White House, 2022). However, data processed from British children could still be accessed by US intelligence services in manners inconsistent with the protection afforded by the UK data protection laws. Only data controllers can take decisions to process personal data outside the UK with a valid transfer mechanism, and where a court in a country outside the EU orders a data processor to transfer or disclose personal data, the data processor must redirect the order to the data controller.<sup>70</sup> Neither Google nor ClassDojo appear to be in complete compliance with this. Such use of data processed from British children could have long-term consequences, such as unexplained suspicion of terrorism or denials of visas.

## Google

Google (2021b) has taken steps to address problems raised. In 2021 Google produced a White Paper on data transfer in Workspace for Education to help customers assess their compliance needs relating to transfers of their EU personal data (Google for Education, 2021b). Measures have been taken in respect of encryption (including client-side encryption – currently in beta), access controls and providing customers the option to specify a 'data region' depending on the type of Workspace agreement they have. Google also uses EU and UK Standard contractual clauses (SCCs).<sup>71</sup>

Customers<sup>72</sup> can elect to have their data stored in the EU if they choose a paid-for version of Workspace for Education.<sup>73</sup> It is unlikely that many schools have taken this option and it is unclear whether this would prevent data being transferred in all circumstances.

The French CNIL ruled on 4 January 2022 that measures put in place by Google are not effective insofar as none of them

---

prevent access possibilities of US intelligence services or render these accesses ineffective. As such, with this transfer of data, the company undermines the level of personal data protection of data subjects as guaranteed in Article 44 of the GDPR. (CNIL, 2022)

---

**The Danish government announced a ban on Google's services in schools in July 2022, in part because its Chromebook laptops and cloud-based Google Workspace**

**software suite ‘does not meet the requirements’ of the GDPR. At issue is that no data flow agreement is yet in operation to replace the EU-US Privacy Shield.<sup>74</sup>**

## ClassDojo

The Privacy Policy has a section headed, ‘What if I’m not in the US?’, which states that ClassDojo is hosted and operated in the USA and that if you use the app from the UK, you may be transferring your personal information from UK jurisdiction to the USA. ClassDojo (2022d) says they ‘have ensured that appropriate safeguards are in place to ensure an adequate level of protection for the rights of data subjects based on the adequacy of the receiving country’s data protection laws’, presumably referring to the standards of the now invalidated EU-US Privacy Shield.<sup>75</sup>

ClassDojo also says that by using the service you consent to storage of your data in the USA and acknowledge that different data protection laws may apply and so ClassDojo may be compelled to disclose your personal information to US authorities. Those ‘different data protection laws’ are not specified, but our research finds that under the FERPA (34 CFR § 99.31),<sup>76</sup> student education records may be shared: to comply with a judicial order or lawfully issued subpoena; with appropriate officials in cases of health and safety emergencies (surely relevant to the present pandemic); and with State and local authorities, within a juvenile justice system, pursuant to specific State law (U.S. Department of Education, 2021).

**The International Data Processing Addendum that schools outside the USA are required to sign when they contract with ClassDojo (2021a, Clause 11) includes ‘European specific provisions’. These detail mechanisms for transfers of personal data from the EU or UK to countries which do not ensure an adequate level of data protection under the EU or UK GDPR.<sup>77</sup>**

## Summary of Problem 4

- **The Dutch investigations identified a series of high data protection risks with Google Workspace for Education including lack of purpose limitation, lack of transparency, no legal basis for Google to process the data, and missing or problematic privacy controls. Further, they claim that Google is really the data controller rather than the processor. Google has since made some improvements, but we believe these have not also been implemented in the UK.**
- **ClassDojo also claims in its contract with schools that the school is the data controller responsible for ClassDojo’s data processing while ClassDojo is the data processor; however, for some aspects of its processing we believe ClassDojo is in fact the data controller and should be registered with the ICO.**
- **Both Google and ClassDojo include vague statements in their contracts with schools, creating a difficulty in determining, for example, the applicable laws. Both products provide a right for schools to audit their data processing, but this would be far too costly for any school.**
- **Both products fail to comply with regulation regarding the transfer of personal data collected from British children to the USA: Google has taken steps which the French data protection authority has ruled ineffective; the Danish government has announced a ban on Google Workspace and Chromebooks in their schools.**

---

## Recommendation 4: Facilitate and coordinate rights-respecting contracts between schools and EdTech providers

- The ICO should clarify that the data controller and processor are determined by the actual technical control over data processing as stipulated in the UK GDPR. They should place the burden of proof on EdTech providers in accurately describing their role (both in their contracts with schools and their privacy policies) with regards the personal data collected, be it as data controllers, joint controllers (with schools) or data processor.
  - EdTech services operating as data controllers (e.g., ClassDojo) must register themselves on the ICO database of data controllers, and ICO should find a means of ensuring compliance.
  - The default settings of any applications offered to a child to use in their learning at school or home must offer high privacy protection, i.e., privacy by default. Where a child can access further digital services through use of a school-approved service, the default high privacy protection should extend to these services. These high privacy settings should preclude children's education data being processed to target advertisements, for commercial profiling or for developing commercial products and services.
  - The ICO should review and update its guidance on overseas data transfers and issue specific guidance to schools. Children's education data should not be transferred to or stored in a country, such as the USA, that does not offer the same level of protection as the UK GDPR.
  - To resolve the 'David and Goliath' problem of some 30,000 schools individually tasked with negotiating complex contracts with EdTech companies and understanding opaque privacy notices, government could negotiate with EdTech providers to produce standard contracts, benchmark standards and default settings for schools that comply with the UK GDPR and meet educational needs.
  - The DfE and devolved ministries should conduct and publish periodic audits of EdTech platforms and other EdTech applications used in UK schools and assess them for compliance with data protection law, regulation and guidance.
-

## Conclusions

The two case studies examined in this report have different business models and influence children's education in different ways. As will have become clear, the devil is in the detail, for both products offer benefits, and are valued in the schools that use them.

However, both Google Classroom and ClassDojo create an easy pathway for children to move unwittingly from privacy-respecting to data-harvesting digital spaces during their learning at school or home. Both make it near impossible for schools or children (or their parents or caregivers) to understand how much of their data, including sensitive or biometric data, is collected from them by EdTech or how and why it is processed and shared more widely within the data ecosystem (Problem 1). We find evidence that children's education is being used for profit in ways that could result in commercial exploitation (Problem 2) by the very EdTech companies claiming to put children's interests first.<sup>78</sup> The critical question is whether, in today's digital world, children can learn without being datified, surveilled, sorted and profited from. The expectation that it is for the government to determine the nature and purposes of children's education is being overtaken by a fast-globalising EdTech sector that increasingly shapes what happens in the classroom with little public consultation or oversight. For example, Google is able 'to monitor and regulate how data are being exchanged, and how functionalities and their associated practices are integrated in the classroom experience' and Google's API 'actively configures pedagogy as a controllable activity and the classroom as a programmable space' (Perotta et al., 2021, p. 103).<sup>79</sup>

Given the problems of lack of transparency, purpose limitation, identification of the data controller and other problems documented in this report, we find it likely that Google Classroom and ClassDojo do not comply with data protection (Problem 3). As stated at the outset of this report, although we chose to focus on two prominent EdTech providers for this investigation, other EdTech companies appear to raise similar problems of transparency, clarity, mistaken assessment of their processing roles and so forth. Rectifying the situation in children's best interests is difficult because the opacity of EdTech companies' privacy policies and legal terms makes it almost impossible for schools and children to counter or renegotiate how companies process data from children.

The current market power of major (mainstream) EdTech and limited guidance issued by the DfE (2022b) means that individual schools cannot properly manage the use of a child's data because they do not fully understand what is collected, for what purpose and how it is used, and they perceive that they have little choice but to accept contractual terms from EdTech companies (Turner et al., 2022). In some contracts, it is difficult to determine in which countries the laws or legal systems apply. Schools do not have the capability or funding to be able to conduct proper audits. It is therefore difficult to see how a school could audit a company's processing to ensure it was done solely in accordance with the school's instructions. This results in schools not knowing if they have full control over how EdTech providers process data from children nor how to rectify any difficulties (Problem 4). Meanwhile, children rarely have the opportunity to refuse the EdTech decisions taken by their school.<sup>80</sup>

In conclusion, schools are contractually responsible (as the data controller) for their students' data processing undertaken by largely unaccountable EdTech companies who

vastly outstrip them in scale, power and resources to negotiate. Further, the overwhelming scale of data collection and the complex nature of the privacy policies and governance systems prevents children, their families, caregivers and schools from understanding and assessing the risk of using EdTech products. To relieve the near-impossible burden placed on the school, parent and caregiver or child to ensure that their data and rights are protected, more of this burden should be shifted to the businesses profiting from EdTech and away from the schools who do not have the budget, capacity or technical/legal skills required.

Meanwhile, although we had hoped and expected that the Age Appropriate Design Code would represent the mechanism by which children's rights rather than profit would dictate uses of children's education data, it seems that the exact phrasing of the law, or arguably the ICO's interpretation of the law, is sufficiently confusing for companies to continue their processing of education data relatively unimpeded by the code. Prompt and firm action led by government is urgently needed to assess and reframe policies, contracts and data use in ways that prioritise child rights principles – best interests, evolving capacity, privacy, freedom from commercial exploitation and surveillance, data protection and data subject rights, and a renewed focus on what matters for education itself. The overarching principle should be that commercial interests must not trump children's best interests. Enacting this principle in policy and practice would promote mutual benefits, resolving conflicts between the underlying interests of children, government and business regarding the uses to which children's data are put.

**We recommend that the government should use the Data Reform Bill as an opportunity to provide clear, accessible and relevant child rights respecting regulation. This would lead to a true pro-innovation approach enabling companies operating in the UK to maximise the benefits of data processed from children in educational contexts for all and with minimised risks to children's safety, privacy and life prospects. This could facilitate an attractive data regime founded on children's best interests and thus trustworthy.**

## Looking ahead

Our analysis contributes to those asking fundamental questions about EdTech's influence on the social and pedagogical agenda within schools, the use of teacher and student labour to create data and information for companies for 'free' ('surveillance capitalism' (Gleason & Heath, 2021; Zuboff, 2019)), the gradual reduction of privacy through surveillance of faces, places, movements and activity of both teachers and students alike, and the potential long-term adverse impacts of education data on their future prospects long after they have left education. We are also concerned that the concentration of children's educational data in the hands of EdTech companies may prevent data being used by other government agencies and the civil society sector in the best interests of children. This is a missed opportunity likely to impede the development of privacy-preserving solutions for education data, open-data innovation and collaborative solutions to benefit children's learning, especially but not only within the non-profit sector.

Meanwhile, EdTech is expanding. During 2021 Google advanced its ambitions to develop Workspace for Education and Google Classroom into a wrap-around learning management system, developing the ability to track student engagement 'such as which



students submitted an assignment or commented on a post on a particular day' (Lazare, 2021). Google is increasing efforts to provide educational content (e.g., 'Google Arts & Culture' (Google, n.d.-a) and 'CS First' – 'a free computer science curriculum that makes coding easy to teach and fun to learn' (Google for Education, n.d.-a; Lazare, 2021). It is rolling out adaptive learning technology to enable teachers to create interactive assignments and provides students with real-time feedback (Cormie, 2022; Kiecza, 2022).<sup>81</sup>

Alongside this, educational content and tools provided by third parties are integrated through the Classroom API and there are already hundreds of third-party operators linked to Google Classroom,<sup>82</sup> some of which involve virtual or augmented reality.<sup>83</sup> As it provides ever more educational content, automated and adaptive learning and management systems, bringing third-party apps into its Classroom environment, it seems that soon, students and teachers will never need to leave the Classroom environment. This would give Google further control over children's education, and further access to their data (Perrotta et al., 2021).<sup>84</sup>

Less is known about ClassDojo although its future plans include expansion in the metaverse.<sup>85</sup> More broadly, the future direction of EdTech travel appears to be towards applying artificial intelligence to shaping the content of lessons, teaching and grading 'facts' and, even, determining the accuracy and grading of 'critical thought'. Meanwhile, extended, augmented and virtual-reality education environments and applications are being developed (Jang et al., 2021) and embryonic ethics standards emerging (Mangina, 2021).<sup>86</sup>

It is surely a priority that government should keep emerging technologies in education under regular review. Equally important is that the ICO should invest in expertise specific to the domain of education, regularly review emerging technologies used or proposed for use in education and their potential risks and their impacts on both the individual child and children and provide clear and timely guidance for schools accordingly.

While technological innovation often outpaces regulation, it is open to EdTech businesses to resolve the problems identified as a matter of the design of their products and services; we invite them to do so, hoping that the analysis in this report illuminates their task. While there are both promising as well as problematic signs of change within the industry, we conclude that greater government and regulator intervention are required to re-empower schools and children to benefit from education data in ways that serve valuable educational, safeguarding and administrative purposes.

# Annex 1: Data processed by Google Classroom and ClassDojo

**Table 1 Data processed by Google Classroom**

Customer data in core services - primarily governed by the Education Privacy Notice			
What data?	For what purpose?	Grounds?	Shared with?
<p>Anything submitted, stored, sent or received through core services by either the student or the school</p> <p><b>'Personal information'</b>: when a Google Workspace for Education account is created the school provides Google with certain personal information about its students and educators including:</p> <ul style="list-style-type: none"> <li>• user's name</li> <li>• email address</li> <li>• password</li> </ul> <p>Schools can add:</p> <ul style="list-style-type: none"> <li>• user's secondary email address (e.g., personal email)</li> <li>• phone number</li> <li>• physical address</li> </ul> <p>Users can add information 'such as':</p> <ul style="list-style-type: none"> <li>• an additional phone number</li> <li>• a profile photo</li> <li>• gender (?)</li> <li>• date of birth (?)</li> </ul> <p>Things the child creates including e.g.</p> <ul style="list-style-type: none"> <li>• Emails</li> <li>• Forms</li> <li>• Sheets</li> <li>• Documents</li> <li>• Photos</li> <li>• Videos</li> </ul>	<ul style="list-style-type: none"> <li>• To provide core services</li> <li>• To determine account type</li> <li>• For authentication purposes</li> </ul> <p>Customer Data in the Workspace for Education Agreement at paragraph 5.2 is limited to the provision of services and technical support services or as otherwise instructed by the Customer.</p> <p><i>Google will not process Customer Data for Advertising purposes or serve Advertising in the Services. Google has implemented and will maintain administrative, physical and technical safeguards to protect Customer Data as further described in the Data Processing Agreement</i></p>	<p>Contract: Processing according to the school's instructions</p>	<p>Google states: 'We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:</p> <ul style="list-style-type: none"> <li>• <b>With your school's admin:</b> Your admin and resellers who manage your Workspace account will have access to your information, including your password and information stored in your account.</li> <li>• <b>With your consent:</b> We'll share personal information outside of Google when we have your consent.</li> <li>• <b>For external processing:</b> We may share personal information with our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our <a href="#">Privacy Policy</a>, the <a href="#">Google Cloud Privacy Notice</a>, and any other appropriate confidentiality and security measures.</li> <li>• <b>For legal reasons:</b> We may also share personal information if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary for legal reasons, including complying with enforceable governmental requests and protecting you and Google.' <p>If admin settings set by school permit, child can share information including their name and photo with others and publicly e.g., comments on YouTube, reviews in Google Play. Child's friends can also share the child's personal information if they have it and settings permit</p> </li></ul>
Service data in core services - primarily governed by Education Privacy Notice with reference to Cloud Privacy Notice			
'Activity' while using core services		<ul style="list-style-type: none"> <li>• Legitimate interest</li> <li>• Contract</li> </ul>	Service data is shared with third parties for various reasons.

		<ul style="list-style-type: none"> <li>• Consent</li> </ul>	<p>Lists of sub-processors here:  <a href="https://workspace.google.com/intl/en/terms/subprocessors.html">https://workspace.google.com/intl/en/terms/subprocessors.html</a></p> <p>The Sub-processor does not have access to Customer Data stored or processed by the Services. The Sub-processor only has access to Customer Data if Customer explicitly elects to share Customer Data in the course of a support case (e.g., screenshots).</p>
<p>How the child views and interacts with content</p>			
<p>People with whom the child communicates or shares data</p>			
<p>Other details about the child's usage of the service</p>			
<p>Information about the child's:</p> <ul style="list-style-type: none"> <li>• apps</li> <li>• browsers (including browser type)</li> <li>• devices (device type)</li> <li>• operating system</li> <li>• settings</li> </ul>			
<p>Unique identifiers</p> <ul style="list-style-type: none"> <li>• mobile number</li> </ul>			
<p>Location information 'as determined by various technologies such as IP address and GPS'</p>			
<p>Information about the interaction of apps with the service</p>			
<p>Other data as detailed in the <a href="#">Google Cloud Privacy Notice</a></p>	<ul style="list-style-type: none"> <li>• to enable the provision of cloud services provide technical and professional services improve online support and to communicate</li> <li>• protect you, our users and the public and Google</li> <li>• comply with legal obligations</li> <li>• other purposes with your consent</li> </ul>	<ul style="list-style-type: none"> <li>• performance of contract</li> <li>• complying with legal obligations</li> <li>• pursuing legitimate interests in respect of Google and third parties in the interests of providing cloud services and providing and improving other services you request</li> </ul>	<p>Data can be shared with a wide variety of third parties outside Google by consent for instance where a third party app is used with administrators and authorized resellers where external processing is undertaken by affiliates, trusted business or persons based on Google's instructions or where necessary for legal reasons.</p>

Customer data in additional services - primarily governed by Google's privacy policy

What data?	For what purpose?	Grounds?	Shared with?
<ul style="list-style-type: none"> <li>• name</li> <li>• password</li> <li>• telephone number (optional)</li> <li>• payment info (optional)</li> </ul>	<ul style="list-style-type: none"> <li>• To create a Google account</li> <li>• Maintain and improve services</li> <li>• develop new services</li> <li>• provide personalized services including content and ads</li> <li>• measure performance</li> <li>• communicate with you</li> <li>• protect Google, our users and the public</li> </ul> <p>Activity is collected, among other reasons, to recommend a YouTube video you might like</p> <ul style="list-style-type: none"> <li>• to protect against abuse</li> <li>• to provide advertising and research services on their behalf</li> </ul>	<p>With consent</p> <p>When pursuing legitimate interests which are set out in some detail:</p> <ul style="list-style-type: none"> <li>• Providing, maintaining and improving our services to meet the needs of our users</li> <li>• Developing new products and features that are useful for our users</li> <li>• Understanding how people use our services to ensure and improve the performance of our services</li> <li>• Customizing our services to provide you with a better user experience</li> <li>• Marketing to inform users about our services</li> <li>• Providing advertising, which keeps many of our services free (and when ads are personalized, we ask for your consent)</li> <li>• Detecting, preventing or otherwise addressing fraud, abuse, security or technical issues with our services</li> <li>• Protecting against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law, including disclosing information to government authorities</li> <li>• Performing research that improves our services for our users and benefits the public</li> <li>• Fulfilling obligations to our partners like developers and rights holders</li> <li>• Enforcing legal claims, including investigation of potential violations of applicable Terms of Service</li> <li>• When we are providing a service you have asked for under a contract</li> <li>• Complying with legal obligations, for example, a request from a government</li> </ul>	<p>The Privacy Policy also sets out the following bases for sharing information:</p> <ul style="list-style-type: none"> <li>• Where the user gives consent e.g., when leaving comments on a YouTube channel</li> <li>• With domain administrators</li> <li>• Personal information may be provided to affiliates, for example, service providers who help with customer support</li> <li>• For legal reasons</li> <li>• Under legal reasons the following paragraph appears: <i>We may share non-personally identifiable information publicly and with our partners – like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies</i></li> </ul>
<p><b>Content you create, upload or receive from others such as:</b></p> <ul style="list-style-type: none"> <li>• Emails</li> <li>• Photos and videos</li> </ul>			

- Docs and spreadsheets
- Comments you make on YouTube videos, in maps, on photos, etc.

- Information about the apps, browsers and devices used to access Google
- Unique identifiers, browser types and settings, device types and settings
- Operating system
- Mobile network information including carrier name and phone number and application version number

Interaction of apps, browsers and devices with Google services includes IP address, crash reports, system activity and the date, time and referrer URL of your request

**Your activity**

- terms you search for
- videos you watch
- views and interactions with ads
- voice and audio information
- purchase activity
- people with whom you communicate or share content
- activity on third party sites and apps that use our services
- chrome browsing history you've synced with your Google account

**Call and messaging information if account used to make, receive calls or send/receive messages includes:**

phone number, calling-party number, receiving-party number, forwarding numbers, sender and recipient email address, time and date of calls and messages, duration of calls, routing information, and types and volumes of calls and messages

**Location information**

**Publicly accessible information – e.g. newspaper**

--	--	--	--

**Table 2 Data processed by ClassDojo**

What data?	Why processed?	By whom?	Legal basis?	Shared with?
First and last name	Establishing one's identity within a school community, or for support needs/responding to surveys	ClassDojo, from data given by the user or teacher on the website or app	Legitimate interest and performance of contract	SendGrid in the USA to send friendlier emails
App or product username	To allow a student to log in and have an account	ClassDojo, from the student when registering on the website or app	Legitimate interest and performance of contract	N/A
Password	To allow users to log in and have an account – student passwords can be reset by teachers when needed	ClassDojo, from the user when registering on the website or app	Legitimate interest and performance of contract	N/A
Mobile device ID	To help identify the types of devices used, to improve the product, and to diagnose issues/bugs	Automatically collected from the device when using the app	Legitimate interest and performance of contract	N/A
Age	To determine if we need parental consent for students to share personal information with ClassDojo	ClassDojo, from the user when registering on the website or app	Legitimate interest, performance of contract, compliance with legal obligations	Not applicable (N/A)
Language information	To provide the service in the user's preferred language	From the device's language settings and/or website browser settings or user choice	Legitimate interest and performance of contract	SendGrid in the USA, to send emails in preferred language
School address	To create connections within a school community among teachers, parents, students and school leaders; to ensure users are in the correct schools	By teachers on the website or app during sign-up	Legitimate interest and performance of contract	
Local school district ID number	To improve quality of the names and addresses of US schools, for school features e.g., school start and end dates to improve teacher usability & School Directory management	Acquired by ClassDojo from MDR Education, one of their service providers	N/A	N/A
Photos, videos, documents, drawings or audio files	Letting users communicate with each other; for students, letting them share their classwork on a digital portfolio with their teacher(s) and parent(s)	By the website or app through product features e.g., messaging, class story, school story, portfolios	Legitimate interest and performance of contract	N/A
IP address - to estimate a coarse geolocation	Transmit data back to the requesting browser or mobile client. Provide information necessary for operations of our servers e.g., security and quality of service; geolocate requests to improve the product for users	Through all server requests from web and mobile clients	Legitimate interest and performance of contract	N/A
Browser details	To provide a working ClassDojo experience tailored to the user's browser	From all server requests from web clients and mobile clients using a web agent	Legitimate interest and performance of contract	N/A
Access time	To improve our product knowledge and for improving marketing emails and notifications delivery	Automatic, based on website or app usage	Legitimate interest and performance of contract	N/A

Page views	To improve our product knowledge and for improving marketing emails and notifications delivery	Automatic, based on website or app usage	Legitimate interest and performance of contract	N/A
Referring URLs	To improve our product knowledge and for improving marketing emails and notifications delivery	Automatic, based on website or app usage	Legitimate interest and performance of contract	N/A
Clicks	To improve our product knowledge about how people use our products, and to better deliver marketing emails to users based on their actual usage	Automatic, based on website or app usage	Legitimate interest and performance of contract	N/A
Click paths	To improve our knowledge about how people use our products, to better deliver marketing emails to users based on their actual usage	Automatic, based on website or app usage	Legitimate interest and performance of contract	N/A
Active/engagement time	To improve our knowledge about how people use our products, to better deliver marketing emails to users based on their actual usage	Automatic, based on website or app usage	Legitimate interest and performance of contract	N/A
Behavioral data / feedback <sup>87</sup>				

## Annex 2: Dutch investigation of Google G Suite (Enterprise) for Education

In 2019 the University of Groningen and the Amsterdam University of Applied Sciences commissioned Privacy Company to conduct a variety of DPIA on the use of G Suite Education and G Suite (Enterprise) for Education in a university setting (Nas & Terra, 2021a, p. 17). The Dutch DPIAs (Nas & Terra, 2021a, 2021b) drew on combined legal and technical knowledge and research and identified a number of high data protection risks. The reports recommended mitigating measures for Google and for universities.

In respect of both customer and service (diagnostic) data, Privacy Company found:

- i) Lack of purpose limitation
- ii) Lack of transparency
- iii) No legal ground for Google or the Universities to process data
- iv) Missing privacy controls
- v) Privacy unfriendly default settings
- vi) The use of multiple Google accounts resulting in data spilling over between education and personal accounts
- vii) Lack of control over sub-processors

They concluded that:

- i) Because of the lack of transparency and purpose limitation, Google did not qualify as a data processor for the processing of any of the personal data it collects in and about the use of G Suite (Enterprise) for Education.<sup>88</sup>
- ii) Google was in fact a data controller or joint controller with the University and could not successfully claim any legal ground for the processing as required by Article 6 GDPR.

Google explained that default privacy settings are more privacy friendly for children in K12 settings. There are several key differences for K12 schools which the authors of the report identify throughout. These are mainly that the Ad personalisation settings are off by default, and default settings for additional services are turned off in K12 Workspace for Education and cannot be turned on by the end user (child, teacher or parent) but could be permitted by an administrator (Nas & Terra, 2021a, p. 14). However, the authors of the report concluded that the main problems relating to purpose limitation, transparency, the role of Google and exercise of data subject rights are identical for all Google Workspace editions regardless of the type of organisation (Nas & Terra, 2021a, p. 10).

The conclusion in respect of K12 schools in the Netherlands is that individual schools must conduct an additional individual risk analysis to determine the risks for children, bearing in mind the following key issues:



- i) Teachers may be storing (unnecessary) additional sensitive data from the pupil administration system in Google Workspace such as exam results, study paths, learning materials, educational monitoring data, and pictures and videos of pupils (although with parental consent).
- ii) Google does not use personal data about the viewing and surfing behaviour of children for advertising but may use it for other purposes which are not clearly specified and may vary depending on the services used at the time.
- iii) Where data is sent unencrypted to be processed in the USA, even if EU data storage is chosen, it gives rise to potential privacy infringements. This is a particular risk for diagnostic data and can cause sensitive personal information to be disclosed.
- iv) Information contained in the child's workspace account may remain with the child for a long period of time leading to future schools deriving conclusions from the data without the child or parent/guardian being aware.
- v) Where consent is used as a basis of processing, for example in additional services, children tend to simply click 'yes'.
- vi) By 9-12 years old, children may start to create their own Google accounts. To protect children against the risk that Google will use the data about the behaviour of the child for commercial purposes, schools should prevent pupils from using a personal Google account in school, by prohibiting simultaneous log-in with a private and a school Google account.
- vii) Until Google becomes a processor rather than controller for Chromebook and Chrome browser, recommended privacy settings identified by the report should be implemented.<sup>89</sup>
- viii) By the ages of 12-16 the above risks apply, and children also have more autonomy over their technology. It is almost inevitable that they will have a private Google account. Children using Android devices are required to create a Google account. For children of this age the difference between a core Service and an additional Service is incomprehensible. Schools should take steps to educate both parents and children about why additional services are blocked on the school account and what the privacy risks are for children.

As a consequence of this intensive exercise undertaken by the Dutch, Google made various changes to some policies (see e.g., the introduction of control access to Google services by age (Google, 2022a)) and some guarantees were given as to purpose limitation. Technical work to change the system architecture is apparently under way.

A second consequence was the production of a support package by Dutch organisations SURF, SIVON and Kennisnet to explain to institutions how best to use Google products (SURF, 2021b). This includes instructions on how to take immediate steps in respect of data protection, a technical manual for systems administrators, and an Education specific DPIA guide for Google Workspace for Education (SURF, 2021b).

**We have been unable to find a comprehensive, similar published document in respect of the use of Google products within education in the UK.**

## Annex 3: Instructions for Schools Administrators on how to customise additional Google services in Google Workspace and their respective terms of service

Service	Description		
AppSheet	Create powerful mobile and web applications in a no-code development environment.	<a href="#">Terms</a>	<a href="#">Help</a>
Applied Digital Skills	Ready-to-use video lessons teach digital skills that have immediate, real-life application.	<a href="#">Terms</a>	<a href="#">Help</a>
Assignments	Quickly and securely create, analyze, and grade coursework, while helping students learn more effectively. Note: Assignments is a <a href="#">core service</a> for Google Workspace for Education Fundamentals and Google Workspace for Education Plus editions.	<a href="#">Terms</a>	<a href="#">Help</a>
Blogger	Share your life online with a blog—it's quick and easy.	<a href="#">Terms</a>	<a href="#">Help</a>
Brand Accounts	Set up and manage your business or brand through an account that is not publicly linked to your Google Account. Use it with certain services, such as YouTube or Google My Business, to create an online presence.	<a href="#">Terms</a>	<a href="#">Help</a>
Campaign Manager 360	Simplifies how campaigns are run, from media planning to reporting.	Requires written agreement	<a href="#">Help</a>
Chrome Web Store	Browse for, purchase, and deploy cloud applications.	<a href="#">Terms</a>	<a href="#">Help</a>
Classroom	Streamline assignments, boost collaboration, and foster seamless communication to make teaching more productive and meaningful. Note: Classroom is a <a href="#">core service</a> for Google Workspace for Education Fundamentals and Google Workspace for Education Plus editions.	<a href="#">Terms</a>	<a href="#">Help</a>
CS First	A computer science curriculum for students ages 9–14.	<a href="#">Terms</a>	<a href="#">Help</a>
FeedBurner	Create and manage custom RSS feeds.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Ad Manager	Streamline your ad management functions with advanced targeting and more.	Requires written agreement	<a href="#">Help</a>
Google Ads	Display your ads on Google and our advertising network.	<a href="#">Terms</a>	<a href="#">Help</a>
Google AdSense	Place Google ads on your website and earn revenue.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Alerts	Monitor the web for interesting new content.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Analytics	Get rich insights into your website traffic and marketing effectiveness.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Arts & Culture	Google Arts & Culture features content from over 2000 leading museums and archives.	<a href="#">Terms</a>	<a href="#">Help</a>

Google Bookmarks	Access your bookmarks on any computer. Use Lists to share them with friends.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Books	Search the full text of books.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Chrome Sync	Synchronize your bookmarks, browser preferences, and browser theme on multiple computers.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Cloud Platform	Grow your business with our secure storage, powerful compute, and integrated data analytics products. (Note: This replaces the service on/off setting for the Google Developers Console).	<a href="#">Terms</a>	<a href="#">Help</a>
Google Colab	Write and execute Python, right in your browser.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Data Studio	Turn your data into easy-to-read charts and interactive reports.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Developer	Documentation and resources for APIs and developer products, including Google Developer profiles.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Domains	Find, buy, transfer, and manage your domains.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Earth	Explore the world, right in your browser.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Fi	A wireless service that helps you get a high-quality connection wherever you are—at home, on-the-go, or even abroad. Available only to people who live in the U.S in <a href="#">eligible locations</a> .	<a href="#">Terms</a>	<a href="#">Help</a>
Google Groups	Create and participate in public discussion groups.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Maps	View maps and directions.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Messages	Messages is a simple messaging app that keeps you connected with the people who matter most. Text anyone from anywhere across devices.	<a href="#">Terms</a>	<a href="#">Help</a>
Google My Business	Help get your business found on Google.	<a href="#">Terms</a>	<a href="#">Help</a>
Google My Maps	Create, share, and publish custom maps.	<a href="#">Terms</a>	<a href="#">Help</a>
Google News	Comprehensive up-to-date news coverage, aggregated from sources all over the world.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Pay	Google Pay is the fast, simple way to pay online or make contactless payments with your phone.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Photos	Store and share photos with Google Photos.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Play	Get the latest apps, games, music, movies, TV, and news for all your devices.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Play Console	Offer Android applications that you develop to the rapidly growing Android user base.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Public Data Explorer	Explore with the Google Public Data Explorer to create visualizations of public data, link to them, or embed them in their own webpages.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Search Console	Get Google's view of your site.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Takeout	Back up and download the data in your Google Account.	<a href="#">Terms</a>	<a href="#">Help</a>
Google Translate	Instantly translate words, phrases, and web pages between English and over 100 other languages.	<a href="#">Terms</a>	<a href="#">Help</a>

Google Trips	Includes all trip details from your email, combined with a destination guide and day planner. Provided on your phone, independent of connectivity.	<a href="#">Terms</a>	<a href="#">Help</a>
Individual storage	Allow end users to purchase additional storage for Google Drive.	<a href="#">Terms</a>	<a href="#">Help</a>
Location History	Control location history and reporting.	<a href="#">Terms</a>	<a href="#">Help</a>
Managed Google Play	Managed Google Play is the content marketplace for Android in the enterprise. Browse and manage apps for your organization.	<a href="#">Terms</a>	<a href="#">Help</a>
Material Gallery	Gallery is a collaborative tool for uploading design work, getting feedback, and tracking revisions – quickly and efficiently.	<a href="#">Terms</a>	<a href="#">Help</a>
Merchant Center	Google Merchant Center lets millions of people discover, explore, and buy your products, and gives you different ways to get the right products to the right customers.	<a href="#">Terms</a>	<a href="#">Help</a>
Partner Dash	Quickly access applications hosted by Google partners.	<a href="#">Terms</a>	<a href="#">Help</a>
Pinpoint	Research tool that helps journalists and academics explore and analyze large collections of documents.	<a href="#">Terms</a>	<a href="#">Help</a>
Play Books Partner Center	Promote your books online through Google Books.	Requires sign-up	<a href="#">Help</a>
Programmable Search Engine	Create a customized search experience for your community.	<a href="#">Terms</a>	<a href="#">Help</a>
QuestionHub	Question Hub is a tool that enables creators to create richer content, by creating content to address unanswered questions.	<a href="#">Terms</a>	<a href="#">Help</a>
Scholar Profiles	Track citations to your articles.	<a href="#">Terms</a>	<a href="#">Help</a>
Search Ads 360	Manage and optimize your pay-per-click ads and keywords across all major search engines.	Requires written agreement	<a href="#">Help</a>
Search and Assistant	Use your account on Google Search and Google Assistant to see personal results, get better speech recognition, and access additional features. <a href="#">Learn more</a>	<a href="#">Terms</a>	<a href="#">Help</a>
Socratic	Learning app, powered by Google AI, helps students understand school work at a high school and university level. <a href="#">Learn more</a>	<a href="#">Terms</a>	<a href="#">Help</a>
Studio	Manage rich media production and workflow with this tool designed for creative agencies.	Requires written agreement	<a href="#">Help</a>
Third-party App Backups	Make third-party app backups available to users in your organization.	<a href="#">Terms</a>	<a href="#">Help</a>
Tour Creator	Create and publish virtual-reality tours.	<a href="#">Terms</a>	<a href="#">Help</a>
Web and App Activity	Save and manage your search activity and enable customized experiences in Search, Maps, and Google Assistant.	<a href="#">Terms</a>	<a href="#">Help</a>
YouTube	Watch, upload, and share videos, and participate in in-app chat. Not available in all regions. <a href="#">Learn more</a>	<a href="#">Terms</a>	<a href="#">Help</a>

## References

- 5Rights Foundation. (2021). *Risky by design*. Retrieved 31 July 2022 from [riskyby.design/introduction](https://riskyby.design/introduction)
- Age Check Certification Scheme Ltd. (2021). *Age Appropriate Design Certification Scheme (AADCS)*. Retrieved 10 June 2022 from <https://ico.org.uk/for-organisations/age-appropriate-design-certification-scheme-aadcs>
- All About 3rd Grade. (2016). *Using ClassDojo for Behavior Management*. Retrieved 29 June 2022 from [https://www.allabout3rdgrade.com/2016/09/using-class-doj-for-behavior-management\\_15.html](https://www.allabout3rdgrade.com/2016/09/using-class-doj-for-behavior-management_15.html)
- Arizton. (2021). *EdTech Market - Global Outlook & Forecast 2022-2027*. Retrieved 11 August 2022 from <https://www.arizton.com/market-reports/edtech-market>
- Ashman, G. (2019, 22 January). *Class Dojo*. Retrieved 11 August 2022 from <https://gregashman.wordpress.com/2019/01/22/class-doj>
- Attorney General of the State of New Mexico. (2021). *Press Release - Attorney General Hector Balderas Announces Landmark Settlements with Google Over Children's Online Privacy*. Retrieved 11 August 2022 from [https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/Attorney\\_General\\_Hector\\_Balderas\\_Announces\\_Landmark\\_Settlements.pdf](https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/Attorney_General_Hector_Balderas_Announces_Landmark_Settlements.pdf)
- Austrian Data Protection Authority. (2022). *The Austrian Data Protection Authority Google Analytics Decision*. Retrieved 9 June 2022 from [https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics\\_EN\\_bk.pdf](https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf)
- Barassi, V. (2020). *Child Data Citizen: How Tech Companies Are Profiling Us from before Birth* (1 ed.). MIT Press. Retrieved 11 August 2022 from [https://mitpress.mit.edu/books/child-data-citizen?\\_ga=2.147312311.1208907863.1624138438-898542324.1621987361](https://mitpress.mit.edu/books/child-data-citizen?_ga=2.147312311.1208907863.1624138438-898542324.1621987361)
- Barran, D. (2021). *Amendment 67 - Skills and Post-16 Education Bill [HL] - Report (2nd Day) (Continued) - in the House of Lords at 7:15pm on 21 October 2021*. <https://www.theyworkforyou.com/lords/?id=2021-10-21c.379.0&s=certification#g380.1>
- Barran, D. (2022). *Education: Standards - Department for Education written question - answered on 23 February 2022*. Retrieved 3 March 2022 from <https://www.theyworkforyou.com/wrans/?id=2022-02-09.HL6145.h>
- Belgian Data Protection Authority (2022). *Complaint relating to Transparency & Consent Framework*. Retrieved 11 August 2022 from <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf>
- Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). *On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?* Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, Virtual Event, Canada. Retrieved 11 August 2022 from <https://doi.org/10.1145/3442188.3445922>

- Brogan, T. (2022, 27 January). Edtech market set to reach \$605.40 by 2027. Retrieved 11 August 2022 from <https://edtechnology.co.uk/latest-news/edtech-market-set-to-reach-605-40-by-2027>
- Chen, R., Kraemer, K. L., & Sharma, P. (2009, 2009/02/01). Google: The World's First Information Utility? *Business & Information Systems Engineering*, 1(1), 53-61. <https://doi.org/10.1007/s12599-008-0011-6>
- Clark, D. (2022a). *Monthly number of downloads of Google Classroom in the United Kingdom from January 2015 to September 2021*. Retrieved 11 August 2022 from <https://www.statista.com/statistics/1266735/uk-google-classroom-downloads>
- Clark, D. (2022b). *Most downloaded educational mobile apps in the UK 2021*. Statista. Retrieved 30 June 2022 from <https://www.statista.com/statistics/1266710/uk-most-downloaded-education-apps>
- ClassDojo. (2018a). *Additional Terms by User Type*. Retrieved 10 June 2022 from <https://www.classdojo.com/en-gb/terms/?redirect=true#additional-terms-by-user-type>
- ClassDojo. (2018b). *ClassDojo - How personal information is collected, its purpose, and how it's protected*. Retrieved 11 August 2022 from <https://docs.google.com/spreadsheets/d/19NhiUx1gARgg6bcClOfwZLbtEA3pkiT7xH2V Cc7bqGo/edit#gid=0>
- ClassDojo. (2018c, 2 November). *Premium Features Terms*. Retrieved 11 June 2022 from <https://www.classdojo.com/premium-features-terms>
- ClassDojo. (2018d, 2 November). *Terms of Service*. Retrieved 8 June 2022 from <https://www.classdojo.com/en-gb/terms?redirect=true>
- ClassDojo. (2021a). *ClassDojo International Data Processing Addendum (Revision February 2021)*. Retrieved 30 May 2022 from <https://static.classdojo.com/docs/DPA/2021-05-classdojo-int-dpa-scc.pdf>
- ClassDojo. (2021b, February). *Student Data Privacy Addendum*. Retrieved 10 June 2022 from <https://static.classdojo.com/docs/DPA/2021-05-classdojo-student-data-dpa.pdf>
- ClassDojo. (2022a, 28 January). *ClassDojo Privacy Policy*. Retrieved 10 June 2022 from <https://www.classdojo.com/en-gb/privacy/?redirect=true#classdojo-privacy-policy>
- ClassDojo. (2022b, 28 January). *Privacy Policy*. Retrieved 10 June 2022 from <https://www.classdojo.com/en-gb/privacy>
- ClassDojo. (2022c). *Transfer of Personal Data to the U.S.* Retrieved 10 June 2022 from <https://classdojo.zendesk.com/hc/en-us/articles/360053338371-Transfer-of-Personal-Data-to-the-US->
- ClassDojo. (2022d, 28 January). *What if I'm not in the US?* Retrieved 10 June 2022 from <https://www.classdojo.com/en-gb/privacy/?redirect=true#what-if-im-not-in-the-us>
- ClassDojo. (n.d.-a). *Bring every family into your classroom*. Retrieved 11 August 2022 from <https://www.classdojo.com/en-gb/?redirect=true>
- ClassDojo. (n.d.-b). *ClassDojo Plus FAQ*. Retrieved 10 June 2022 from <https://classdojo.zendesk.com/hc/en-us/articles/360018137732>

- ClassDojo. (n.d.-c). *How does Google Login for students work?* Retrieved 11 August 2022 from <https://classdojo.zendesk.com/hc/en-us/articles/360018868571>
- ClassDojo. (n.d.-d). *Make Google Classroom more effective.* Retrieved 11 August 2022 from <https://www.classdojo.com/googleclassroom>
- ClassDojo. (n.d.-e). *Safety and privacy.* Retrieved 11 June 2022 from <https://classdojo.zendesk.com/hc/en-us/articles/115004762046>
- ClassDojo. (n.d.-f). *Student Data Privacy Addendum.* Retrieved 9 June 2022 from <https://classdojo.zendesk.com/hc/en-us/articles/360062517931-Student-Data-Privacy-Addendum-DPA->
- ClassDojo. (n.d.-g). *What are "Student Accounts" and "Outside School Child Accounts?"*. Retrieved 11 August 2022 from <https://classdojo.zendesk.com/hc/en-us/articles/4413231512205-What-are-Student-Accounts-and-Outside-School-Child-Accounts->
- ClassDojo. (n.d.-h). *What's ClassDojo?* Retrieved 9 June 2022 from <https://www.classdojo.com/en-gb/about/?redirect=true>
- ClassDojo Point System* (n.d.). Retrieved 30 June 2022 from <https://i.pinimg.com/736x/8e/82/48/8e8248163b5a60728801c9a2f769d48b-behaviour-management-behavior.jpg>
- CNIL. (2019). *Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société X.* Retrieved 5 June 2022 from <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038032552>
- CNIL. (2022a, 6 January). *Cookies: GOOGLE fined 150 million euros.* Retrieved 11 August 2022 from <https://www.cnil.fr/en/cookies-google-fined-150-million-euros>
- CNIL. (2022b). *Google Analytics et transferts de données: comment mettre son outil de mesure d'audience en conformité avec le RGPD?* Retrieved 10 June 2022 from <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/google-analytics-et-transferts-de-donnees-comment-mettre-son-outil-de-mesure-daudience-en-conformite>
- Common Sense Media. (2020, March). *ClassDojo - Website review.* Retrieved 11 August 2022 from <https://www.commonsense.org/education/website/classdojo>
- Connolly, K. (n.d.). *Overcoming ADHD Inside the Classroom.* Retrieved 11 August 2022 from <https://www.classdojo.com/en-gb/stories/overcoming-adhd-inside-the-classroom>
- Cormie, A. (2022, 9 June 2022). *Let's get personal: adaptive learning tech and education.* Retrieved 11 August 2022 from <https://www.blog.google/outreach-initiatives/education/adaptive-learning-technology>
- Council of Europe. (2020). *Children's Data Protection in an Education setting - Guidelines.* Retrieved 11 August 2022 from <https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b>
- Court of Justice of the European Union. (2017). *Asociación Profesional Elite Taxi v Uber Systems Spain (CJ0434).* Retrieved 11 August 2022 from <https://curia.europa.eu/juris/document/document.jsf?text=&docid=198047&doclang=EN>

- Court of Justice of the European Union. (2020). *Schrems II (ECLI:EU:C:2020:559)*. Retrieved 11 August 2022 from <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageInd ex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12312155>
- Day, E. (2021). *Governance of data for children's learning in UK state schools*. Digital Futures Commission - 5Rights Foundation. Retrieved 11 August 2022 from <https://digitalfuturescommission.org.uk/beneficial-uses-of-education-data>
- DCMS. (2021). *The UK Safety Tech Sector: 2021 Analysis*. Retrieved 11 August 2022 from [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach ment\\_data/file/989753/UK\\_Safety\\_Tech\\_Analysis\\_2021\\_-\\_Final\\_-\\_190521.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach ment_data/file/989753/UK_Safety_Tech_Analysis_2021_-_Final_-_190521.pdf)
- DCMS. (2022, 23 June). *Data: a new direction - government response to consultation*. Retrieved 30 June 2022 from <https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation>
- Defend Young Minds. (2021, 13 July). *How to Set Up Google FAMILY LINK Parental Controls*. Retrieved 10 June 2022 from <https://www.defendyoungminds.com/post/how-to-set-up-google-family-link-parental-controls>
- defenddigitalme. (2022, 20 June). *Data Protection Reform and a Reality Check*. Retrieved 30 June 2022 from <https://defenddigitalme.org/2022/06/20/data-protection-reform-and-a-reality-check>
- Department for Education (DfE). (2018). *Data protection: a toolkit for schools (DFE-00119-2018)*. Retrieved 11 August 2022 from [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach ment\\_data/file/747620/Data\\_Protection\\_Toolkit\\_for\\_Schools\\_OpenBeta.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach ment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf)
- DfE. (2019). *Realising the potential of technology in education*. Retrieved 11 August 2022 from <https://www.gov.uk/government/publications/realising-the-potential-of-technology-in-education>
- DfE. (2020). *Schools to benefit from education partnership with tech giants*. Retrieved 11 August 2022 from <https://www.gov.uk/government/news/schools-to-benefit-from-education-partnership-with-tech-giants>
- DfE. (2021). *Guidance - Remote education good practice (withdrawn on 30 March 2022)*. <https://www.gov.uk/government/publications/remote-education-good-practice/remote-education-good-practice>
- DfE. (2022a). *Complete the school census - Statutory requirement, data sharing and regulations*. Retrieved 11 August 2022 from <https://www.gov.uk/guidance/complete-the-school-census/statutory-requirement-data-sharing-and-regulations>
- DfE. (2022b). *Guidance - Providing remote education: guidance for schools*. Retrieved 11 August 2022 from <https://www.gov.uk/government/publications/providing-remote-education-guidance-for-schools>
- DiGiacomo, D. K., Greenhalgh, S., & Barriage, S. (2021). How Students and Principals Understand ClassDojo: Emerging Insights. *TechTrends: for leaders in education & training*, 1-13. <https://doi.org/10.1007/s11528-021-00640-6>



- EDPB. (2019, 21 January). *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*. Retrieved 1 June 2022 from [https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros\\_en](https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en)
- EDPB. (2020). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR - Version 1.0. Adopted on 2 September 2020*. Retrieved 11 August 2022 from [https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and\\_en](https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en)
- EDPB. (2021a). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 2.0)*. Retrieved 11 August 2022 from [https://edpb.europa.eu/system/files/2021-07/eppb\\_guidelines\\_202007\\_controllerprocessor\\_final\\_en.pdf](https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf)
- EDPB. (2021b, 18 June). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0)*. Retrieved 5 June 2022 from [https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer\\_en](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en)
- EDPS. (2022). *Data protection and use of cloud by public sector: the EDPS initiates and participates in the 2022 Coordinated Enforcement Action of the EDPB*. Retrieved 11 August 2022 from [https://edps.europa.eu/press-publications/press-news/press-releases/2022/data-protection-and-use-cloud-public-sector-edps\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2022/data-protection-and-use-cloud-public-sector-edps_en)
- EdSurge. (n.d.). *Classroom Management - ClassDojo*. Retrieved 10 June 2022 from <https://www.edsurge.com/product-reviews/classdojo>
- Education Act 1996. Retrieved 11 August 2022 from <https://www.legislation.gov.uk/ukpga/1996/56/contents>
- EESC. (2021). *AI in Europe: not all decisions can be reduced to ones and zeros, says the EESC*. Retrieved 11 August 2022 from <https://www.eesc.europa.eu/en/news-media/news/ai-europe-not-all-decisions-can-be-reduced-ones-and-zeros-says-eesc>
- Eidens, A. (2021, 4 August). *Why Grit is More Important in Your Kids Than IQ (And One Simple Way to Teach It)*. Retrieved 11 August 2022 from [https://biglifejournal-uk.co.uk/blogs/blog/why\\_grit](https://biglifejournal-uk.co.uk/blogs/blog/why_grit)
- Erick, K. (2021). *Google Sued Over Purported Privacy Violations for Real-Time Bidding Auctions*. Law Street. Retrieved 6 May from <https://lawstreetmedia.com/news/tech/google-sued-over-purported-privacy-violations-for-real-time-bidding-auctions>
- European Commission. (2021). *Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council*. Official Journal of the European Union. Retrieved 10 June 2022 from <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0915&from=EN>
- European Parliament. (2020). *The CJEU judgment in the Schrems II case*. Retrieved 11 August 2022 from

[https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS\\_ATA\(2020\)652073\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf)

- European Union. (2002). *Treaty Establishing the European Community (OJC325, 24/12/2002 P. 0033 - 0184 - OJC340; 10/11/1997 P. 0173 - Consolidated version)*. Retrieved 10 June 2022 from <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12002E/TXT&from=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). *Coronavirus: UK schools will get tech support from Google and Microsoft*. Computer Weekly. Retrieved 11 August 2022 from <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. Retrieved 11 August 2022 from <http://www.lawbriefpublishing.com/product/gdprforschools>
- ForHumanity. (2021). *Certification scheme is designed for “Information Society Services (ISS) likely to be accessed by Children”*. Retrieved 5 June 2022 from <https://forhumanity.center/children-s-code>
- French National Data Protection Commission (CNIL). (2022, 10 February). *Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply*. Retrieved 9 June 2022 from <https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply>
- Gibbs, S. (2013, 28 October). *Mozilla’s Lightbeam Firefox tool shows who’s tracking your online movements*. Retrieved 11 August 2022 from <https://www.theguardian.com/technology/2013/oct/28/mozilla-lightbeam-tracking-privacy-cookies>
- Gleason, B., & Heath, M. K. (2021). Injustice Embedded in Google Classroom and Google Meet: A Techno-Ethical Audit of Remote Educational Technologies. *Emergency Remote Education: methodological, technological, organizational and policy issues, 29*(2). <https://doi.org/10.17471/2499-4324/1209>
- Gold, A. (2021, 13 December). *Google settles children’s privacy suits brought by New Mexico*. Retrieved 11 August 2022 from <https://www.axios.com/2021/12/13/google-new-mexico-children-privacy>
- Google. (2021a, 24 September). *Data Processing Amendment to Google Workspace and/or Complementary Product Agreement (Version 2.4)*. Retrieved 11 August 2022 from [https://workspace.google.com/terms/dpa\\_terms.html](https://workspace.google.com/terms/dpa_terms.html)
- Google. (2021b). *Google Cloud’s Approach to the New EU Standard Contractual Clauses*. Retrieved 6 June 2022 from [https://services.google.com/fh/files/misc/gc\\_new\\_eu\\_scc.pdf](https://services.google.com/fh/files/misc/gc_new_eu_scc.pdf)
- Google. (2021c, 24 September). *Google Workspace Admin Help - Privacy compliance and records for Google Workspace and Cloud Identity*. Retrieved 11 August 2022 from

<https://support.google.com/a/answer/2888485?hl=en-GB#zippy=%2Chow-to-opt-in-to-the-data-processing-amendment-dpa%2Chow-to-indicate-if-european-data-protection-law-applies-to-you-and-provide-related-information%2Chow-to-accept-the-hipaa-business-associate-amendment>

Google. (2022a). *Google Workspace Admin Help - Control access to Google services by age*. Retrieved 9 June 2022 from <https://support.google.com/a/answer/10651918>

Google. (2022b). *Privacy & Terms - List of Services & Service Specific Additional Terms*. Retrieved 11 August 2022 from <https://policies.google.com/terms/service-specific>

Google. (2022c, 10 February). *Privacy Policy*. Retrieved 11 August 2022 from <https://policies.google.com/privacy?hl=en-US>

Google. (2022d). *Terms of Service*. Retrieved 11 August 2022 from <https://policies.google.com/terms>

Google. (n.d.-a). *Google Arts & Culture*. Retrieved 10 June 2022 from <https://artsandculture.google.com>

Google. (n.d.-b). *Google Workspace Admin Help - Monitor usage and security with reports*. Retrieved 11 August 2022 from <https://support.google.com/a/answer/6000239?hl=en>

Google. (n.d.-c). *Manage your child's Google Account with Family Link*. Retrieved 10 June 2022 from <https://support.google.com/families/answer/7103262?hl=en>

Google. (n.d.-d). *Safety Center - Families*. Retrieved 11 August 2022 from <https://safety.google/intl/en-GB/families>

Google Cloud. (2021, 24 September). *Data Processing and Security Terms (Customers)*. Retrieved 8 June 2022 from <https://cloud.google.com/terms/data-processing-terms>

Google Cloud. (2022a, 30 March). *Google Cloud Platform, Workspace, Cloud Identity & Implementation Services: EU Model Contract Clauses (Controller-to-Processor) - UK*. Retrieved 10 June 2022 from <https://cloud.google.com/terms/sccs/uk-c2p>

Google Cloud. (2022b, 4 April). *Google Cloud Platform, Workspace, Cloud Identity & Implementation Services: EU Standard Contractual Clauses (Module 2: Controller-to-Processor)*. Retrieved 10 June 2022 from <https://cloud.google.com/terms/sccs/eu-c2p>

Google Cloud. (2022c, 4 April). *Google Cloud Platform, Workspace, Cloud Identity & Implementation Services: EU Standard Contractual Clauses (Module 3: Processor-to-Processor)*. Retrieved 10 June 2022 from <https://cloud.google.com/terms/sccs/eu-p2p>

Google Cloud. (2022d, 4 April). *Google Cloud Platform, Workspace, Cloud Identity & Implementation Services: EU Standard Contractual Clauses (Module 3: Processor-to-Processor, Google Exporter)*. Retrieved 10 June 2022 from <https://cloud.google.com/terms/sccs/eu-p2p-google-exporter>

Google Cloud. (2022e, 4 April). *Google Cloud Platform, Workspace, Cloud Identity & Implementation Services: EU Standard Contractual Clauses (Module 4: Processor-to-Controller)*. Retrieved 10 June 2022 from <https://cloud.google.com/terms/sccs/eu-p2c>

Google Cloud. (2022f, 20 April). *Google Cloud Privacy Notice*. Retrieved 9 June 2022 from <https://cloud.google.com/terms/cloud-privacy-notice>

- Google Cloud. (2022g, 15 March). *Google Contracting Entity*. Retrieved 11 June 2022 from <https://cloud.google.com/terms/google-entity>
- Google Cloud. (2002h). *Estimate Data Access audit log costs*. Retrieved 8 August 2022 from <https://cloud.google.com/bigtable/docs/audit-log-estimate-costs#:~:text=The%20average%20audit%20size%20is,charged%20%240.01%2FGiB%20for%20storage>
- Google for Education. (2020, 10 December). *Tech Toolkit for Families and Guardians*. YouTube. Retrieved 10 June 2022 from <https://www.youtube.com/playlist?list=PLP7Bvyb3ap44MII5eZ8RqY9VtuELuJ4eT>
- Google for Education. (2021a, 20 September). *Google Workspace for Education Terms of Service*. Retrieved 11 August 2022 from [https://workspace.google.com/terms/education\\_terms.html](https://workspace.google.com/terms/education_terms.html)
- Google for Education. (2021b). *Safeguards for international data transfers with Google Workspace and Workspace for Education*. Retrieved 11 August 2022 from [https://services.google.com/fh/files/misc/workspace\\_and\\_workspace\\_edu\\_safeguards\\_for\\_international\\_data\\_transfers.pdf](https://services.google.com/fh/files/misc/workspace_and_workspace_edu_safeguards_for_international_data_transfers.pdf)
- Google for Education. (2022a). *Choose the edition that's right for your institution*. Retrieved 11 August 2022 from [https://edu.google.com/intl/ALL\\_uk/workspace-for-education/editions/compare-editions/](https://edu.google.com/intl/ALL_uk/workspace-for-education/editions/compare-editions/)
- Google for Education. (2022b). *Where teaching and learning come together*. Retrieved 11 August 2022 from [https://edu.google.com/intl/ALL\\_uk/workspace-for-education/classroom/](https://edu.google.com/intl/ALL_uk/workspace-for-education/classroom/)
- Google for Education. (2022c). *Privacy and security centre*. Privacy and security EMEA. Retrieved 11 August 2022 from [https://edu.google.com/intl/ALL\\_uk/why-google/privacy-security/](https://edu.google.com/intl/ALL_uk/why-google/privacy-security/)
- Google for Education. (n.d.-a). *CS First - A computer science curriculum that makes coding easy to teach and fun to learn*. Retrieved 10 June 2022 from <https://csfirst.withgoogle.com/s/en/home#>
- Google for Education. (n.d.-b). *Privacy and security centre*. Retrieved 11 August 2022 from [https://edu.google.com/intl/ALL\\_uk/why-google/privacy-security/](https://edu.google.com/intl/ALL_uk/why-google/privacy-security/)
- Google Workspace. (2022). *Google Workspace for Education Privacy Notice*. Retrieved 11 August 2022 from [https://workspace.google.com/terms/education\\_privacy.html](https://workspace.google.com/terms/education_privacy.html)
- Google Workspace. (n.d.). *Services Summary*. Retrieved 11 August 2022 from [https://workspace.google.com/intl/en/terms/user\\_features.html](https://workspace.google.com/intl/en/terms/user_features.html)
- Gulson, K., Perrotta, C., Williamson, B., & Witzemberger, K. (2021). Should We be Worried about Google Classroom? The Pedagogy of Platforms in Education. *Journal of Professional Learning*. <https://cpl.asn.au/journal/semester-2-2021/should-we-be-worried-about-google-classroom-the-pedagogy-of-platforms-in#.YSWMZfRyDqo.twitter>
- Harris, A. (2016, 9 December). *How Google is Schooling Apple and Microsoft in the Battle for America's Classrooms*. Fast Company. Retrieved 10 June 2022 from <https://www.fastcompany.com/3062958/how-google-is-schooling-apple-and-microsoft-in-the-battle-for-americas-classrooms>

- Hill-Budreau, S. (2022, 27 January). The following came from an article written in June 21. Did this update occur? Retrieved 11 August 2022 from <https://support.google.com/edu/classroom/thread/148067905/the-following-came-from-an-article-written-in-june-21-did-this-update-occur?hl=en>
- IAB. (2021). *IAB Europe's Guide to Contextual Advertising*. Retrieved 11 August 2022 from <https://iabeurope.eu/knowledge-hub/iab-europes-guide-to-contextual-advertising/>
- ICO. (2020). *Age Appropriate Design: A Code of Practice for Online Services*. Retrieved 11 August 2022 from <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>
- ICO. (2021a). *FAQs for education technologies (edtech) and schools*. Retrieved 15 November 2021 from <https://ico.org.uk/for-organisations/childrens-code-hub/additional-resources/faqs-for-education-technologies-edtech-and-schools/>
- ICO. (2021b). *Guide to the General Data Protection Regulation*. Retrieved 11 August 2022 from <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf>
- ICO. (2021c). *Right to be informed*. Retrieved 9 June 2022 from <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/>
- IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children* (2021, 30 November). IEEE. Retrieved 1 May 2022 from <https://ieeexplore.ieee.org/document/9627644/>
- Jang, J., Ko, Y., Shin, W. S., & Han, I. (2021). Augmented Reality and Virtual Reality for Learning: An Examination Using an Extended Technology Acceptance Model. *IEEE Access*, 9, 6798-6809. <https://doi.org/10.1109/ACCESS.2020.3048708>
- Kieczka, D. (2022, 16 March). *Practice sets: a more personal path to learning*. Retrieved 11 August 2022 from <https://blog.google/outreach-initiatives/education/introducing-practice-sets/>
- Konrad, A. (2022, 21 July). *ClassDojo Won Over Classrooms. Now It's on A \$125 Million Mission To Bring Kids To The Metaverse*. Forbes. Retrieved 11 August 2022 from <https://www.forbes.com/sites/alexkonrad/2022/07/21/classdojo-tencent-backed-unicorn-launches-education-virtual-world/?sh=667af86d13ad>
- Krach, S. K., McCreery, M. P., & Rimel, H. (2017, 2017/09/01). Examining Teachers' Behavioral Management Charts: a Comparison of Class Dojo and Paper-Pencil Methods. *Contemporary School Psychology*, 21(3), 267-275. <https://doi.org/10.1007/s40688-016-0111-0>
- Krausová, A. (2018, 09/17). Online Behavior Recognition: Can We Consider It Biometric Data under GDPR? *Masaryk University Journal of Law and Technology*, 12, 161. <https://doi.org/10.5817/MUJLT2018-2-3>
- Krutka, D. G., Smits, R. M., & Willhelm, T. A. (2021). Don't Be Evil: Should We Use Google in Schools? *TechTrends: for leaders in education & training*, 1-11. <https://doi.org/10.1007/s11528-021-00599-4>

- Lafer, G. (2015). *Taylorizing education for profit*. Association of Professors of the University of Ottawa. Retrieved 10 June 2022 from <https://apuo.ca/taylorizing-education-profit-gordon-lafer/>
- Lazare, M. (2021, 17 February). *A peek at what's next for Google Classroom*. Retrieved 11 August 2022 from <https://blog.google/outreach-initiatives/education/classroom-roadmap/>
- Lindh, M., & Nolin, J. (2016). Information we collect: Surveillance and privacy in the implementation of Google Apps for Education. *European Educational Research Journal*, 15(6), 644-663. <https://doi.org/10.1177/1474904116654917>
- Livingstone, S., Pothong, K., & Atabey, A. (2021). *Addressing the problems and realising the benefits of processing children's education data - Report on an expert roundtable*. Digital Futures Commission - 5Rights Foundation. Retrieved 11 August 2022 from <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/11/Roundtable-report-25112-final.pdf>
- Lupton, D. (2021, 2021/07/03). 'Honestly no, I've never looked at it': teachers' understandings and practices related to students' personal data in digitised health and physical education. *Learning, Media and Technology*, 46(3), 281-293. <https://doi.org/10.1080/17439884.2021.1896541>
- Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, 19(5), 780-794. <https://doi.org/10.1177/1461444816686328>
- Mangina, E. (2021). *Extended Reality (XR) Ethics in Education (The IEEE Global Initiative on Ethics of Extended Reality Report)*. IEEE. Retrieved 11 August 2022 from <https://standards.ieee.org/wp-content/uploads/import/governance/iccom/xr-in-education.pdf>
- Manolev, J., Sullivan, A., & Slee, R. (2019, 2019/01/02). The datafication of discipline: ClassDojo, surveillance and a performative classroom culture. *Learning, Media and Technology*, 44(1), 36-51. <https://doi.org/10.1080/17439884.2018.1558237>
- Mukherjee, S. et al. (2021). *Child Rights Impact Assessment - A tool to realise children's rights in the digital environment*. Digital Futures Commission. 5Rights Foundation. Retrieved 11 August 2022 from <https://digitalfuturescommission.org.uk/wp-content/uploads/2022/06/Child-Rights-Impact-Assessment.pdf>
- Muller, C. (2021). *Opinion of the European Economic and Social Committee on Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts (COM(2021) 206 final - 2021/106 (COD))*. EESC. Retrieved 11 August 2022 from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021AE2482#:~:text=There%20is%20no%20place%20in,such%20as%20at%20the%20workplace>
- Mumsnet. (2021). *I've had enough of the ClassDojo*. Retrieved 11 August 2022 from [https://www.mumsnet.com/Talk/am\\_i\\_being\\_unreasonable/4257126-i-ve-had-enough-of-the-class-dojo](https://www.mumsnet.com/Talk/am_i_being_unreasonable/4257126-i-ve-had-enough-of-the-class-dojo)

- Murphy, H. (2022). *Facebook patents reveal how it intends to cash in on metaverse*. Retrieved 11 August 2022 from <http://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647>
- Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of "Personally Identifiable Information". *Communications of the ACM*, 53(6), 24-26.  
<https://doi.org/10.1145/1743546.1743558>
- Nas, S., & Terra, F. (2021a). *DPIA on the use of Google G Suite (Enterprise) for Education (15 July 2020, update 12 March 2021)*. Privacy Company. Retrieved 11 August 2022 from <https://www.sivon.nl/app/uploads/2021/06/SIVON-Updated-G-Suite-for-Education-DPIA-12-March-2021-v1.2.pdf>
- Nas, S., & Terra, F. (2021b). *Update DPIA report Google Workspace for Education (2 August)*. Privacy Company. Retrieved 11 August 2022 from <https://www.surf.nl/files/2021-08/update-dpia-report-2-august-2021.pdf>
- Nemorin, S. (2017). Post-panoptic pedagogies: the changing nature of school surveillance in the digital age. *Surveillance and Society*, 15(2), 239-253.  
<http://eprints.lse.ac.uk/83311/1/Nemorin-Post%20pan-optic%20pedagogies.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>
- Perrotta, C., Gulson, K. N., Williamson, B., & Witzemberger, K. (2021, 2021/01/01). Automation, APIs and the distributed labour of platform pedagogies in Google Classroom. *Critical Studies in Education*, 62(1), 97-113.  
<https://doi.org/10.1080/17508487.2020.1855597>
- Perspective Economics, & University of East Anglia. (2020). *Safer technology, safer users: the UK as a world-leader in Safety Tech*. Department for Digital, Culture, Media & Sport. Retrieved 11 August 2022 from <https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech>
- Persson, J. (2020). *The State of Data 2020: Mapping a Child's Digital Footprint Across England's State Education Landscape*. Retrieved 11 August 2022 from <https://defenddigitalme.org/research/the-state-of-data-2020/>
- 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>
- Revolution Professional. (2019). *Data Protection Impact Assessment (ClassDojo)*. Retrieved 11 August 2022 from <https://greenfield.dudley.sch.uk/wp/wp-content/uploads/2020/05/Data-Protection-Impact-Assessment-ClassDojo.pdf>
- Saner, E. (2018, 30 April). *ClassDojo: do we really need an app that could make classrooms overly competitive?* The Guardian. Retrieved 11 August 2022 from <https://www.theguardian.com/education/shortcuts/2018/apr/30/classdojo-do-we-really-need-an-app-that-could-make-classrooms-overly-competitive>
- Sawers, P. (2022, 18 July). *Denmark bans Chromebooks and Google Workspace in schools over data transfer risks*. TechCrunch. Retrieved 11 August 2022 from

[https://guce.techcrunch.com/copyConsent?sessionId=3\\_cc-session\\_3e3cfce2-7cb7-40c5-ab93-6e4523e730ce&lang=en-US](https://guce.techcrunch.com/copyConsent?sessionId=3_cc-session_3e3cfce2-7cb7-40c5-ab93-6e4523e730ce&lang=en-US)

Shephard, B. (2021, 22 July). *The New Rise of Contextual Advertising*. Retrieved 11 August 2022 from <https://www.forbes.com/sites/forbesagencycouncil/2021/07/22/the-new-rise-of-contextual-advertising/>

Singer, N. (2014, 16 November). *Privacy Concerns for ClassDojo and Other Tracking Apps for Schoolchildren*. The New York Times. Retrieved 11 August 2022 from <https://www.nytimes.com/2014/11/17/technology/privacy-concerns-for-classdojo-and-other-tracking-apps-for-schoolchildren.html>

SIVON. (n.d.). *The cooperation of and for primary and secondary education*. Retrieved 11 May 2022 from <https://www.sivon.nl/>

Smith, A. (2020, 27 August). *Google's privacy settings so confusing even its own engineers couldn't turn them off, lawsuit shows*. The Independent. Retrieved 11 August 2022 from <https://www.independent.co.uk/tech/google-privacy-settings-engineers-location-tracking-phone-a9691046.html>

Soroko, A. (2016). No Child Left Alone: The ClassDojo App. *Our Schools/Our Selves, Spring*, 63-75. Retrieved 11 August 2022 from [https://www.researchgate.net/profile/Agata-Soroko/publication/304627527\\_No\\_child\\_left\\_alone\\_The\\_ClassDojo\\_app/links/5775607508ae1b18a7dfdeed/No-child-left-alone-The-ClassDojo-app.pdf](https://www.researchgate.net/profile/Agata-Soroko/publication/304627527_No_child_left_alone_The_ClassDojo_app/links/5775607508ae1b18a7dfdeed/No-child-left-alone-The-ClassDojo-app.pdf)

Speed, R. (2022, 30 May). *Dutch public sector gets green light to use Google Workspace*. The Register. [https://www.theregister.com/2022/05/30/google\\_workspace\\_dutch\\_government/](https://www.theregister.com/2022/05/30/google_workspace_dutch_government/)

Statista. *Worldwide visits to Google.com from September 2021 to February 2022*. <https://www.statista.com/statistics/268252/web-visitor-traffic-to-googlecom/#:~:text=In%20February%202022%2C%20search%20platform,the%20biggest%20online%20companies%20worldwide.>

Stoilova, M., Livingstone, S., & Nandagiri, R. (2020, 2020-11-10). Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy [Article]. *Media and Communication*, 8(4), 197-207. <https://doi.org/http://dx.doi.org/10.17645/mac.v8i4.3407>

Stoilova, M., Nandagiri, R., & Livingstone, S. (2021, 2021/03/12). Children's understanding of personal data and privacy online – a systematic evidence mapping. *Information, Communication & Society*, 24(4), 557-575. <https://doi.org/10.1080/1369118X.2019.1657164>

SURF. (2021a). *Cooperation provides greater Bargaining Power in Talks with "Big Tech"*. Retrieved 11 August 2022 from <https://www.surf.nl/en/surf-magazine/cooperation-provides-greater-bargaining-power-in-talks-with-big-tech>

SURF. (2021b, 2 August). *Google Workspace for Education support package*. Retrieved 8 June 2022 from <https://www.surf.nl/en/google-workspace-for-education-support-package>

SURF. (n.d.). *SURF is the collaborative organisation for IT in Dutch education and research*. Retrieved 11 August 2022 from <https://www.surf.nl/en>



- Thoppilan, R., Freitas, D., Hall, J., Shazeer, N., Kulshreshtha, A., Cheng, H.-T., Jin, A., Bos, T., Baker, L., Du, Y., Li, Y., Lee, H., Zheng, H., Ghafouri, A., Menegali, M., Huang, Y., Krikun, M., Lepikhin, D., Qin, J., & Le, Q. (2022). *LaMDA: Language Models for Dialog Applications*. Retrieved 11 August 2022 from <https://arxiv.org/pdf/2201.08239.pdf>
- 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. Retrieved 11 August 2022 from <https://digitalfuturescommission.org.uk/beneficial-uses-of-education-data/>
- U.S. Department of Education. (2021, 25 August). *Family Educational Rights and Privacy Act (FERPA)*. Retrieved 10 June 2022 from <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- UNCRC. (2013). *General Comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1) (CRC/C/GC/14)*. Retrieved 11 August 2022 from <https://www.refworld.org/docid/51a84b5e4.html>
- UNCRC. (2021). *General Comment No. 25 on Children's Rights in Relation to the Digital Environment (CRC/C/GC/25)*. Retrieved 11 August 2022 from <https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx>
- United Nations Convention on the Rights of the Child. (1989). United Nations, Treaty Series, vol. 1577, p. 3. <https://www.refworld.org/docid/3ae6b38f0.html>
- United States District Court for the District of New Mexico. (2020). *State of Mexico, ex rel., Hector Balderas, Attorney General of the State of New Mexico v. Google LLC (20 February)*. Retrieved 11 August 2022 from [https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG\\_Balderas\\_Sues\\_Google\\_for\\_Illegally\\_Collecting\\_Personal\\_Data\\_of\\_New\\_Mexican\\_School\\_Children.pdf](https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Sues_Google_for_Illegally_Collecting_Personal_Data_of_New_Mexican_School_Children.pdf)
- US Department of Commerce. (2021, 31 March). *FAQs – EU-U.S. Privacy Shield Program Update*. Retrieved 8 June 2022 from <https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update>
- van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefwaard, T. (2020, 14 Dec. 2020). The Child's Right to Protection against Economic Exploitation in the Digital World. *The International Journal of Children's Rights*, 28(4), 833-859. <https://doi.org/https://doi.org/10.1163/15718182-28040003>
- Walters, R. (2021) UK EdTech sector grows to £3.5bn as demand surges for digital classrooms and AR.FE News. Retrieved 31 July 2022 from <https://www.fenews.co.uk/skills/uk-edtech-sector-grows-to-3-5bn-as-demand-surges-for-digital-classrooms-and-ar/>
- White House. (2022, 25 March). *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*. Retrieved 10 June 2022 from <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/>

- Williamson, B. (2016, 2 September). *A sociotechnical survey of a public sphere platform*. Retrieved 11 August 2022 from <https://codeactsineducation.wordpress.com/2016/09/02/assembling-classdojo/>
- Williamson, B. (2021, 28 May). *Google's plans to bring AI to education make its dominance in classrooms more alarming*. Fast Company. Retrieved 11 August 2022 from <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* (1 ed.) [Report]. Education International Research. Retrieved 11 August 2022 from <https://eprints.qut.edu.au/209028/>
- Williamson, B., & Rutherford, A. (2017). *ClassDojo poses data protection concerns for parents*. Retrieved 11 August 2022 from <http://eprints.lse.ac.uk/76141/>
- Wilson, J. (2021). *Artificial Intelligence and "Social Scoring"*. Retrieved 11 August 2022 from <https://www.eupoliticalreport.eu/artificial-intelligence-and-social-scoring/>
- Young, A. (2020). *Responsible group data for children* (Issue brief no. 4). UNICEF. Retrieved 11 August 2022 from <https://www.unicef.org/globalinsight/media/1251/file/UNICEF-Global-Insight-DataGov-group-data-issue-brief-2020.pdf>
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (1 ed.). PublicAffairs.

## Endnotes

- 
- 1 See DfE (2020), Flinders (2020). For example, Google first launched free software for education in 2006 and low-cost Chromebooks in 2011 (Williamson, 2021). By 2016 Google dominated the K-12 educational landscape in the USA (Harris, 2016). The pandemic resulted in a consolidation of Google's position in the global education 'market' (Lazare, 2021).
- 2 See DfE (2021). This Guidance was subsequently withdrawn and replaced with effect from 29 March 2022. However, the funding and support for schools to use either Google or Microsoft as a platform remained until at least November 2021.
- 3 See <https://www.bleepingcomputer.com/news/security/chrome-use-subject-to-restrictions-in-dutch-schools-over-data-security-concerns>
- 4 See <https://www.itp.net/commsmea/20197-apple-google-and-microsoft-clouds-banned-in-schools-in-germany>
- 5 See <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag>
- 6 See <https://dataethics.eu/the-troublesome-case-of-using-google-in-european-schools>
- 7 As we were researching this report, several European Data Protection Authorities made decisions on aspects of surveillance technologies such as Google Analytics and data transfers (Austrian Data Protection Authority, 2022; French National Data Protection Commission (CNIL), 2022), cookies and IP address collection that will have a far-reaching impact (CNIL, 2022a, 2022b). A recent decision by the Belgian Data Protection Authority (2022) on GDPR issues connected to identifying individual profiles via their IP addresses and real time bidding and advertising may have an impact on Google's data collection practices. Legal action is also underway in the USA (Errick, 2021). We note that the European Data Protection Supervisor (EDPS) initiated and participated in the 2022 Coordinated Enforcement Action launched by the European Data Protection Board (EDPB), focusing on data protection and the use of cloud services by public sector bodies to identify whether a formal investigation is warranted (EDPS, 2022). One aspect under investigation is the controller/processor relationship identified as a particular issue in Google Workspace for Education below.
- 8 See United Nations Convention on the Rights of the Child (1989), UNCRC. (2021).
- 9 See Day, E. (2021), Persson, J. (2020), Stoilova, M., Nandagiri, R., & Livingstone, S. (2021), Turner, S., Pothong, K., & Livingstone, S. (2022); Williamson, B., & Hogan, A. (2020).
- 10 It has been suggested that AI learning companions intended to support students on their lifelong learning journeys 'may result in the perpetual recording of learner failure to the detriment of future progress.' (Luckin et al., 39, quoted in Persson, 2020, para 200).
- 11 The UN Committee on the Rights of the Child (UNCRC) emphasises as fundamental that "the concept of the child's best interests is aimed at ensuring both the full and effective enjoyment of all the rights recognized in the Convention and the holistic development of the child." Respecting the child's best interests as a primary consideration in actions by the state is the first of 15 standards in the AADC (ICO, 2020), and is explained in international law in General Comment 14 (UNCRC, 2013) on Article 3(1) of the UN Convention on the Rights of the Child. Crucially, the best interests concept must be applied holistically and dynamically to the full range of children's rights.
- 12 Department for Education (DfE) (2019), Walters (2021); see also DCMS (2021).
- 13 See Brogan (2022).
- 14 The UK GDPR is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419). It is defined in Section 3(10) of the Data Protection Act 2018 (DPA 2018), supplemented by section 205(4).
- 15 The current proposals appear to weaken not strengthen protections for children's data, although we note the avowed aim of unlocking data for re-use that serve both public and commercial interests. See DCMS. (2022, 23 June) and, for a critique, defenddigitalme. (2022, 20 June).
- 16 For an account of how these are deployed in schools, see Turner, S., Pothong, K., & Livingstone, S. (2022).
- 17 Schools have a statutory obligation to submit school census and individual pupil records under Section 537A of the Education Act 1996.
- 18 Worldwide, Google estimates the number of users of its education products increased from 40 million in 2020 to 150 million in 2021, with over 1 million UK downloads of Google Classroom across the iPhone, iPad and Google Play stores (Clark, 2022a). ClassDojo's website states it is "actively used in 95% of all K-8 schools in the U.S. and 180 countries," (ClassDojo, n.d.-h). Tencent valued ClassDojo in 2021 at \$1.25 bn. See Konrad (2022).
- 19 See DfE (2019).
- 20 Recital 26 UK GDPR.
- 21 Where originality reports are used Google states: 'Google doesn't save the content that you submit for the report and doesn't assume ownership of your content. That content belongs to you and your students. Originality reports search for what is publicly available on the web. They're not permanently stored' (Google for Education, 2022b).
- 22 Note that in this report, a school platform administrator refers to a school-based Google Workspace for Education administrator. Additionally, administrators have access to information about the organisation's Gmail and Google Drive usage, such as the types of email activity, the number of documents created and shared, and how much Drive storage each team member is using. Administrators are also able to assess and control security measures and other administrative issues Google (n.d.-b).
- 23 Article 4(8) UK GDPR defines a processor as 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.

24 Article 4(7) UK GDPR defines a controller as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (subject to certain exceptions in Section 6 DPA 2018).

25 For a detailed analysis see Annex 1, Table 1.

26 DPA paragraph 2.2 applies GDPR definitions. Article 4(1) UK GDPR 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

27 These data are described as 'primarily governed' by the Education Privacy notice because the policy itself refers to multiple additional policies but if there is a conflict the Education Privacy notice takes precedence. For fuller detail, please refer to Annex 1.

28 For a detailed analysis see Annex 1, table 2. See also ClassDojo. (2021a).

29 We have been unable to find out what LEA stands for in available documentation.

30 Behavioral data /feedback is included in the 'Teacher' rather than 'Student' section of the Information Transparency section of the ClassDojo website, unlike the other categories of data in this table (<https://www.classdojo.com/en-gb/transparency/?redirect=true>), but it has been included here because it is data about students, is central to ClassDojo's product, and it is listed as a category of data collected from students in the ClassDojo Student Privacy Addendum; see p.4 in the Addendum (2020, 2021), <https://static.classdojo.com/docs/DPA/2021-05-classdojo-student-data-dpa.pdf>

31 Article 9 UK GDPR processing of special categories of data.

32 ClassDojo's Privacy Policy provides as follows: Information Received from Third Party Sources

We may also obtain information, including personal information, from third-party sources to update or supplement the information you provided or we collected automatically. This may include aggregated anonymous information or certain personal information that may be provided to us. If we receive personal information from third-parties, we will handle it in accordance with this Privacy Policy. If we directly combine information we receive from other third-parties with personal information that we collect through the Service, we will treat the combined information as personal information and handle it in accordance with this Privacy Policy. Additionally, we may use any aggregated anonymous information received by third-parties as set forth below under the heading "[Aggregated Information and Non-Identifying Information] (Privacy Policy 2021 DRAFT)". Local law may require you authorize the third-party to share your information with us before we can acquire it. We do not control, supervise, or respond to how third parties providing your information process your personal information, and any information request regarding the disclosure of your personal information to us should be directed to such third-parties. Please see this chart with the detailed categories of personal information we collect from each user type, including the sources from which the information was collected, the business purpose for which the information was collected, and the third parties with whom we share or disclose personal information for a business purpose.

33 Common Sense Media (2020) notes that this public feature could be problematic and that its effectiveness depends largely on 'responsible and consistent use by teachers'. An article in the New York Times in 2014 said that parents were concerned that ClassDojo can be used as a shame-based tool, and some parents thought Dojo Points should only be shared with specific children and parents and not with the entire class (Singer, 2014). A mother on an online message board complained that every week one or two children 'win the Dojo and get a prize', and that day a child who had defaced another child's clothing had won the prize (Mumsnet, 2021).

34 Although not commenting specifically on educational contexts, the EESC opinion stated that there is "no place in the EU for the scoring of the trustworthiness of EU citizens based on their social behaviour or personality characteristics, irrespective of the actor performing the scoring" (Muller, 2021). Surely this must also apply to educational settings in the UK, Brexit notwithstanding.

35 The pedagogy that underlies ClassDojo is based on ideas that emanate from Californian psychologists Carol Dweck and Angela Duckworth regarding 'growth mindset', grit and character. These are designed to build individual resilience and encourage children to think more about how they approach learning than how well they score in tests (Williamson & Rutherford, 2017; Eidens, 2021, Williamson, 2016). Some researchers criticise the use of rewards and punishments for behaviours as being likely to erode self-motivation and self-regulation (Ashman, 2019).

36 She notes that there is a big difference between assessment of learning, and assessment of behaviour (Soroko, 2016). Lafer (2015) argues that apps like ClassDojo are not based on any kind of insights from pedagogy but on the idea that 'kids are bored at school, but they like video games'."

37 Krausová, A. (2018, 09/17) explains that behavioural based tracking techniques do not require cookies or other explicit identifiers but can instead use methods of pattern recognition applied to activities on an app or environmental peculiarities. She states that "behaviour-based tracking partly corresponds to the definition of behavioural biometrics that seeks to 'quantify behavioural traits exhibited by users and use resulting feature profiles to successfully verify identity'."

38 While advertising and marketing is to some degree being displaced by contextual advertising, the problem remains that children are being exposed to advertising in an educational context. Contextual advertising is a process whereby the content of a webpage is matched to the content of an advertisement, and by using sophisticated artificial intelligence that does not rely on the use of personal data, advertisers are still able to quite accurately guess the characteristics of their audience (IAB, 2021; Shephard, 2021).

39 Even if Google implemented mitigating measures to protect privacy within additional services, some such as YouTube also have social sharing and communication features (e.g., 'like' and comment) (5Rights Foundation, 2021) which allow a user to share the video they created, or viewed, comment and respond to comments on the videos they created or viewed publicly with others. This in turn leads to privacy risks for children who are able to leave reviews, posting their name and avatar next to their activity or through information shared by their friends (Google Workspace, 2022).

40 In this experiment, the two children and one of their parents were asked to walk researchers through their Google Classroom user journey and answer our questions about how they use Google Classroom and the instructions from schools. The Digital Future Commission's research ethics procedure was followed.

- 41 EdTech providers should respect children’s right to protection against economic exploitation (UN Convention on the Rights of the Child, 1989, Article 32) and adhere to the recommendations on how this right applies in the digital environment set out in General Comment 25 (UNCRC, 2021).
- 42 The ICO should implement the recommendations children’s right to protection against economic exploitation in the digital environment prescribed in the General Comment 25 *ibid*.
- 43 Google (2021a, 24 September). These apply if the DPA is accepted by the school. Acceptance only necessary if not incorporated into the Workspace Agreement Google (2021c, 24 September).
- 44 The DPA was amended to ensure compliance with EU standard Contractual Terms (European Commission, 2021).
- 45 Google Workspace for Education Terms of Service 15.16 ‘Conflicting Terms. If there is a conflict between the documents that make up this Agreement, the documents will control in the following order (of decreasing precedence): the Order Form, the Data Processing Amendment, the remainder of the Agreement (excluding the URL Terms), and the URL Terms (other than the Data Processing Amendment)’ (Google for Education, (2021a, 20 September).
- 46 DPIA on the use of Google G Suite (Enterprise) for Education for the University of Groningen and the Amsterdam University of Applied Sciences and Update report by Privacy Company (‘the Dutch DPIAs’). This initial report running to 175 pages was completed in July 2020, reviewed in December 2020 and updated 12 March 2021 (Nas & Terra, 2021a). A further update 46 page report was published on 2 August 2021 (Nas & Terra, 2021b).
- 47 He made this observation on explaining the impact of collaboration between educational institutions in the Netherlands with SURF. (n.d.). and SIVON. (n.d.), see also SURF. (2021a).
- 48 See [https://www.theregister.com/2022/05/30/google\\_workspace\\_dutch\\_government/](https://www.theregister.com/2022/05/30/google_workspace_dutch_government/) for the bespoke arrangement eventually agreed in May 2022 with the Dutch government, and <https://www.bleepingcomputer.com/news/security/chrome-use-subject-to-restrictions-in-dutch-schools-over-data-security-concerns/> for the continuing concerns which mean that Google Search is still banned in Dutch schools
- 49 See <https://techmonitor.ai/policy/privacy-and-data-protection/denmark-google-ban-workspace-chromebook-gdpr>
- 50 See <https://www.itp.net/commsmea/20197-apple-google-and-microsoft-clouds-banned-in-schools-in-germany>
- 51 See <https://dataethics.eu/the-troublesome-case-of-using-google-in-european-schools>
- 52 For an example of the realities facing parents under pressure to consent to data infringements by schools, see Barassi (2020).
- 53 The age of consent to data processing in relation to information society services (‘ISS’) is 13 (Article 8 UK GDPR), in which case the question is whether the child has the competency to make such a decision regarding their data processing.
- 54 The lawfulness of processing is defined under UK GDPR Article 6(1) as: consent, performance of a contract, necessary for compliance with a legal obligation, necessary to protect the vital interests of the data subject of another natural person, performance of a task carried out in the public interest, legitimate interests of the controller. There must be a lawful basis for each basis of processing.
- 55 Under the s123 Data Protection Act 2018 the ICO was required to prepare a code of practice on Age Appropriate Design. The AADC took effect on 2 September 2020. Standard 4 AADC: ‘The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent, and in clear language suited to the age of the child. Provide additional specific ‘bite-sized’ explanations about how you use personal data at the point that use is activated’ (ICO, 2020).
- 56 See Mukherjee et al. (2021).
- 57 Standard 8 IEEE 2089-2021 *ibid*.
- 58 See also Jehovah’s Witnesses, C-25/17, ECLI: EU:C:2018:57 para. 68.
- 59 Google Cloud EMEA means the contracting entity that is Google Cloud Europe, the Middle East, and Africa (Google Cloud, 2022g, 15 March).
- 60 Much of this analysis is based on examining audit logs and available telemetry data to determine the data being collected (Nas & Terra, 2021a).
- 61 This assertion was not accepted by Google DPIA *ibid*. and section 5.4 *ibid*. But it has since agreed to limit the purposes.
- 62 Based on interviews conducted by the Digital Futures Commission it does not appear that these measures have been applied in the UK.
- 63 It could be that ClassDojo only defines the legal basis for data processing carried out by itself as data controller because the school defines the legal basis where the school is controller and ClassDojo is the processor. Nevertheless, the legal bases on ClassDojo’s website illustrate that ClassDojo is a controller at least some of the time.
- 64 International Addendum ClassDojo. (2021a): “Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, LEA is the Controller, ClassDojo is the Processor and that ClassDojo or members of the ClassDojo Group will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” below.”
- 65 No. 480. The DPA 2018 requires every data controller that is processing personal information to register with the ICO and to pay a fee, and the company is then featured in the ICO’s public searchable database. Subject to the problems above in respect of determining whether Google is a processor or controller for the purposes of Core Services, Google has otherwise complied with this requirement and has eight companies registered as controllers in the ICO database.
- 66 “Data Protection Laws and Regulations” are defined in the contract as “all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement” (ClassDojo, 2021a, Section 1).
- 67 As per 7.4 DPA that it maintains at least the following for the Audited Services in order to evaluate the continued effectiveness of the Security Measures: a) certificates for ISO 27001, ISO 27017 and ISO 27018 (the “Compliance Certifications”); and b) SOC 2 and SOC 3 reports produced by Google’s Third Party Auditor and updated annually based on an audit performed at least once every 12 months (the “SOC Reports”). Google may add standards at any time. Google may replace a Compliance Certification or SOC Report with an equivalent or enhanced alternative.

68 Schedule 1: Standard contractual clauses.

69 See European Parliament (2020), US Department of Commerce (2021); see also the EDPB recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (EDPB, 2021b).

70 Article 38 UK GDPR.

71 SCCs means the Customer SCCs and/or SCCs (EU Processor-to-Processor, Google Exporter), as applicable.

SCCs (EU Controller-to-Processor) means the terms at Google Cloud (2022b, 4 April). SCCs (EU Processor-to-Controller) means the terms at Google Cloud (2022e, 4 April). SCCs (EU Processor-to-Processor) means the terms at Google Cloud (2022c, 4 April). SCCs (EU Processor-to-Processor, Google Exporter) means the terms at Google Cloud (2022d, 4 April). SCCs (UK Controller-to-Processor) means the terms at Google Cloud (2022a, 30 March).

72 Here, the term “customer” is used to stay consistent with Google’s terminology in its data descriptions and privacy policies. In the context of this paper, “customer” encompasses EdTech users (e.g., schools, teachers, parents and students) who interact with the service.

73 Based on an estimated 10.5 million children in state education this would cost between US\$31.5-52.5 million at a cost of \$3-\$5 per child per year depending on the edition of workspace chosen. See [www.trustradius.com/products/google-workspace-for-education/pricing](http://www.trustradius.com/products/google-workspace-for-education/pricing)

74 See Sawers (2022).

75 ClassDojo (2022c) notes that although the EU-US Privacy Shield no longer applies they still choose to follow the same standards therein.

76 FERPA is the US Federal law introduced to protect the privacy of students’ educational records in the USA. Beyond FERPA it is possible that wider US national security laws may apply to British students’ personal data stored in the USA as implied in the Trans-Atlantic Data Privacy Framework, White House (2022, 25 March).

77 The provisions refer to standard contract clauses contained in a schedule to the International Data Processing Addendum and where applicable to GDPR Article 49 derogations such as consent or performance of contract as the legal basis for transfer of data (ClassDojo, 2021a).

78 Myriad claims are made about the benefits of some emerging technology. Yet experts generally agree that there is insufficient evidence to be confident of the pedagogical or other benefits of EdTech for a child (Livingstone et al., 2021). Some are concerned that, rather than assisting teachers or reducing their workload, EdTech increases the burden for teachers and parents (Gleason & Heath, 2021; Turner et al., 2021).

79 The strategic aims and purpose of the Classroom Application Programming Interface (API) were stated at launch in 2015 to be to ‘further Google’s services and infrastructure into education, creating an ecosystem of third party apps built on the foundation of Google’s powerful and scalable cloud’ (Perrotta et al., 2021, p. 102).

80 As EdTech companies appear to shift the burden and responsibility for privacy and data protection to individual schools and families (Krutka et al., 2021), there are consequential risks for entrenching discrimination and inequality (Gleason & Heath, 2021).

81 According to the promotional material, Artificial Intelligence (‘AI’) will identify learners’ problems based on information about where a child becomes stuck or gets something wrong. It will then recommend YouTube videos to enable learners to find help and information. It is likely that the data generated from the teachers’ and children’s interactions with these products will be used to train and further develop the AI models.

82 Some of these are endorsed by Google and other products can be linked by schools or teachers through share buttons or data synchronisation (Perrotta et al., 2021). This adds an additional layer of complexity to the privacy and governance structures and further muddies the waters in terms of what is happening to children’s data and the uses to which it is put.

83 “We’re starting with nine partners including Adobe Spark for Education, BookWidgets, CK-12 Foundation, Edpuzzle, IXL, Kahoot!, Nearpod, Newsela and SAFARI Montage, with plans to expand to many more. Here’s an example of how Bookwidgets is using add-ons to make it easier for teachers to assign an activity and students to complete it, without ever leaving Classroom” (Hill-Budreau, 2022).

84 On 16 March 2022 Google announced its intention to launch ‘Practice sets’ as a form of ‘adaptive learning technology’. The video explainer describes how this will enable a teacher to upload their own content into interactive assignments, use the auto grading tool to cut down on grading time, and identify patterns where individual students or groups of students need additional assistance (Kiecza, 2022). For students, this new tool identifies the skills being taught and selects and displays resources (such as YouTube videos) so that ‘when students are struggling to solve a problem, they can get hints through visual explainers and videos’. They also get ‘fun animations and confetti’ to celebrate their success when they get it right. These Practice Sets are linked to Google’s work on Language Models which require large data sets (Thoppilan et al., 2022). Large language models are not without controversy both in terms of the computational power required and consequent environmental costs and the potential to further embed bias and discriminatory practices through using data sets too large to audit (Bender et al., 2021).

85 See Konrad (2022).

86 Noted by the Financial Times, ‘Pupil movements, body poses and nose scrunching are among the flickers of human expression that Meta wants to harvest in building its metaverse, according to an analysis of dozens of patents recently granted to Facebook’s parent company’ (Murphy, 2022).

87 As noted earlier, behavioral data /feedback is included in the ‘Teacher’ rather than ‘Student’ section of the Information Transparency section of the ClassDojo website, unlike the other categories of data in this table. It is listed as a category of data collected from students in the ClassDojo Student Privacy Addendum; see p.4 at <https://static.classdojo.com/docs/DPA/2021-05-classdojo-student-data-dpa.pdf>. The Privacy Addendum does not include details of purposes or legal basis of data processing included for the other categories of data in the Information Transparency section, so these sections have been left blank.

88 The previous version of Workspace for Education.

89 A checklist of settings is provided (Nas & Terra, 2021b).

90 See <https://support.google.com/a/answer/181865#zippy=%2Cturn-services-on-or-off-for-users%2Cimportant-disclaimer%2Cservices-with-an-individual-on-or-off-control,%20accessed%2010/12/21>