Ethical Design for Edtech Platforms - An Analysis of Google Classroom via a Code of Design Practices

Steffano Pereira, Maria Eduarda Rebelo, George Valença

Departamento de Computação – Universidade Federal Rural de Pernambuco (UFRPE)
Praça Farias Neves, 2 - Dois Irmãos – 52.171-900 – Recife – PE – Brazil

{steffano.pereira,eduarda.rebelo,george.valenca}@ufrpe.br

***Abstract. Introduction**: The widespread adoption of EdTech platforms in schools exposes children to significant risks that conflict with their rights under the UN Convention on the Rights of the Child (UNCRC). These risks include the opaque collection and processing of personal data for non-educational purposes, the use of this data for commercial profiling, and a lack of user control, which undermines their rights to privacy and protection from economic exploitation. **Objective:** This paper aims to address these risks by developing a practical ethical design guide. The guide is intended to empower educational institutions to assess and select EdTech platforms that are designed to proactively protect children's rights. **Methodology or Steps**: The guide was developed through a multi-phase process: a review of academic and gray literature to identify best practices, systematic categorization of these practices into ten key areas, and alignment with legal frameworks like Brazil's General Data Protection Law (LGPD) and CONANDA Resolution N° 245. **Results:** The primary result is an ethical design guide composed of 12 actionable practices for evaluating EdTech platforms. The guide's utility is demonstrated through a critical analysis of Google Classroom, highlighting how the framework can identify specific data protection and ethical shortcomings in widely used educational software, thereby providing a tangible tool for fostering safer digital learning environments.*

***Keywords** Edtechs, Ethical Design, Deceptive Design, Platforms*

1. Introduction

The digital environment has become an increasingly integral part of children's lives, offering numerous opportunities for education, socialization, and recreation [Livingstone et al. 2024a]. Although these technologies present significant benefits, they also pose considerable risks to the well-being and rights of young people [Livingstone e Stoilova 2021], making the United Nations Convention on the Rights of the Child (UNCRC) and its core tenet of the "best interests of the child" more relevant than ever in the digital sphere [Assembly e Directorate 1991]. Specifically, the widespread adoption of educational technology (EdTech) platforms introduces critical risks. These include the opaque collection and processing of sensitive student data, the use of these data for commercial profiling beyond educational purposes, and a lack of transparent controls that undermine the ability of children and their guardians to provide meaningful and informed consent [Day 2021, Valença et al. 2024].

Today, the immersion of children and teens in the digital environment is an undeniable reality, marked by increasingly early and comprehensive access to online platforms and services. In Australia, a report shows that 80% of the children surveyed aged 8 to 12 years used one or more social media platforms, despite the minimum age of 13 years stipulated by most of the platforms surveyed [eSafety Commissioner 2025]. Meanwhile, in Brazil 93% of children aged 9 to 17 years use the Internet for common online activities, such as social networks, educational platforms, and instant messaging [Núcleo de Informação e Coordenação do Ponto BR 2024]. The results also show that 83% have their own profiles on these platforms [Núcleo de Informação e Coordenação do Ponto BR 2024], posing risks of unauthorized consent to data collection.

These statistics from both Australia and Brazil underscore the deep penetration of the digital environment into the lives of children. This extensive use, while offering educational opportunities through online platforms, also exposes young people to risks that require careful consideration from the perspective of the best interests of the child, as established in the United Nations Convention on the Rights of the Child [Assembly e Directorate 1991]. To address this challenge, the main contribution of this paper is the development of a comprehensive ethical design guide for EdTech platforms. This guide translates foundational children's rights principles and regulatory mandates into a set of actionable practices for stakeholders, aiming to mitigate the risks inherent in educational technologies and ensure they are designed to proactively safeguard children's well-being and rights.

The remainder of this paper is organized as follows. Section 2 discusses the conceptual foundations of Child Rights by Design and ethical design. Section 3 presents the methodology used to develop the proposed design code. Section 4 outlines key practices identified through our analysis. Section 5 applies our proposed framework to the widely used EdTech platform Google Classroom, analyzing it as a practical case study to discuss our findings. Finally, Section 6 concludes the paper and describes future work.

2. Conceptual Background

2.1. Child Rights By Design

Child Rights by Design (CRbD) can be described as a proactive and principled approach to advocate for the explicit integration of children's rights and best interests into the conception, development, deployment of digital technologies, products and services[1]. Rooted in the United Nations Convention on the Rights of the Child (UNCRC) and further elaborated in the Committee on the Rights of the Child's General Comment No. 25 on childrenś rights in the digital environment, the privacy-by-design driven framework moves beyond reactive safety measures, calling upon innovators, policymakers and businesses to consider the holistic well-being, development, participation, and protection of children from the outset to ensure that the digital world is intentionally shaped to uphold their fundamental rights and promote positive outcomes[2]. The CRbD framework is anchored by eleven distinctive principles, which according to Livingstone [Livingstone e Pothong 2023] are:

[1] Child Rights by Design - 5Rights Foundation | https://childrightsbydesign.5rightsfoundation.com/page/child-rights-by-design/

[2] Convention on the Rights of the Child | https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

1. **Equity and Diversity**: Calls for inclusivity, fair treatment, and provision for diverse needs and circumstances.
2. **Best Interests**: Calls for the inclusion of children's best interests when designing and developing products.
3. **Consultation**: Highlights the need to engage and listen to the children's perspective when designing and developing products.
4. **Age Appropriate**: Highlights the need for developing products that are age-appropriate by design and consider using age assurance.
5. **Responsible**: Addresses the need to comply with legal frameworks, remediation when needed, and conducting a Child Rights Impact Assessment.
6. **Participation**: Reinforces the need to enable children's participation, expression, and access to information.
7. **Privacy**: Reinforces the need for embedded privacy-by-design and data protection in the development and use of digital products.
8. **Safety**: Stresses the need for embedded safety-by-design in product development and use.
9. **Wellbeing**: Seeks to enhance and not harm the health and wellbeing of all children, especially through the use of inclusive design.
10. **Development**: Highlights the need to enable children's learning, free play, sociability, belonging, and their full development.
11. **Agency**: Reinforces how decisions should be made to reduce the development of exploitative features and business models that harm the agency of children users.

Child Rights by Design also aligns itself with requirements presented in most data protection regulations, which aim to secure children's right to privacy. According to Art. 8 of the General Data Protection Regulation (GDPR), specific conditions apply to a child providing consent for technology-based services, stating that *"where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child"* and determining the controller as responsible for making *"reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology"*[3].

2.2. Ethical Design

The ethical implications of technology and design on society have garnered increasing attention from the HCI community, who often explore these issues in their role as researchers and designers. Prior investigations into these technological and social challenges have employed approaches such as critical design, value-sensitive design (VSD), and values at play [Fansher et al. 2018]. Ethical design in software development introduces the idea of creating technology that respects human values, dignity, and societal well-being, going beyond mere usability to consider the moral implications of the developed product. This human-centered approach calls for a strong moral compass in order to build designs that are not only functional but also have a positive impact on users and society. A core principle is respecting the user's autonomy through transparency, informed consent, and providing users with control over their experience and data, as

[3] Art. 8 – GDPR | `https://gdpr-info.eu/art-8-gdpr/`

secured through many data protection regulations such as GDPR and LGPD[4]. Fairness and equity are also paramount, requiring biases and inclusive design to be actively addressed in order to ensure equal opportunities for all users.

Basic ethical design principles include respecting human agency, liberty, and dignity through positive and negative freedoms; ensuring technical robustness and safety via resilience, reliability, and accuracy; upholding privacy and data governance, including data quality, access, and rights; promoting transparency through traceability, explainability, and clear communication; fostering diversity, non-discrimination, and fairness by mitigating bias and ensuring inclusive engagement; prioritizing individual, societal, and environmental wellbeing through sustainable systems and the support of social cohesion and democratic institutions; and establishing accountability through auditability and the minimization and reporting of negative impacts with internal and external governance mechanisms [Lundgren 2023].

Ethical design is a foundational pillar in the process of designing and developing ethically-informed and responsible technology, serving as a collective commitment to user well-being, moving beyond superficial solutions to create genuinely beneficial products. This product development process demands deep-seated, critical reflection. Ethical frameworks, thorough user research, and diverse perspectives are deliberately woven into every stage of development, aiming to uphold fundamental human values in the digital realm. Designing products ethically is the essential catalyst for moving from conversation to action, ensuring technology serves humanity rather than exploiting it. Technologists bear a fundamental moral responsibility to society that requires action beyond mere ethical discourse and corporate social responsibility pronouncements. True responsibility demands a renewed commitment to developing digital products and services that are both functional and purposeful, ultimately enabling child users to thrive and fully realize their potential [Michael 2024].

2.3. Deceptive Patterns

One of the many challenges of modern design is commonly described as deceptive and manipulative patterns, which are design artifacts in user interfaces that impair the autonomy of the end user [Sánchez Chamorro et al. 2023]. These patterns aim to erode user autonomy by obstructing informed choices through manipulative design practices [Kollmer e Eckhardt 2022] that undermine a user's ability to make autonomous and informed decisions, regardless of the designer's intention [Tilsner et al. 2011].

Early academic work on deceptive and manipulative patterns expand beyond simple definitions to develop taxonomies of user interface types, offering rich descriptions for each identified pattern. Brignull's work introduces a classification of 12 distinct deceptive pattern types, exemplified by *Bait-and-Switch*, where users are led to expect one outcome but experience an undesirable alternative, and *Confirmshaming*, which guilt-trips users into opting in [Brignull et al. 2023]. Building on this foundational work, subsequent research introduces deceptive patterns within specific application domains. Zagal et al. lists seven deceptive pattern types prevalent in video games, such as *Pay to Skip*, which monetizes in-game progress, and *Grinding*, which compels users to

[4] Brazil's General Data Protection Law (LGPD) | https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

engage in repetitive tasks [Zagal et al. 2013]. Greenberg et al., for instance, presents the "proxemic"interaction deceptive patterns in systems interacting with physical space, citing examples like the *Attention Grabber* and the *Milk Factor* [Greenberg et al. 2014]. Lastly, Lacey and Caudwell's work accounts for a potential "cuteness" factor in home robotics functioning as a deceptive pattern [Lacey e Caudwell 2019].

Mathur et al. introduce a taxonomy of deceptive patterns to demonstrate how manipulative design practices exploit users' cognitive biases and influence their decision-making [Mathur et al. 2019]. These patterns typically present unequal choices, highlighting options that benefit the service provider while obscuring alternatives that would better serve the user. This is especially common in consent interfaces, where tactics such as Trick Questions and Privacy Zuckering are employed.

Often referred to as dark patterns (a term we avoid here due to potential racial connotations), these strategies guide users toward predetermined outcomes by concealing the mechanisms of influence -whether through cognitive manipulation or visual emphasis. Additionally, deceptive patterns can foster false beliefs through misstatements or omissions. For example, shopping websites may use fake countdown timers or hide critical information to prevent users from making fully informed decisions. Such tactics include *Sneaking*, *Hidden Subscriptions*, and *Hidden Costs*.

2.4. Related Work

Pothong et al. examine the challenges and methodologies employed by designers in integrating children's rights into the development of digital products and services. Through facilitated workshops utilizing a tool informed by "Playful by Design" principles, the study explored designers' interpretations and implementation of these rights, with a specific focus on the right to play. The results suggest a tendency among designers to prioritize safety and age-appropriateness, while encountering difficulties in concurrently upholding children's rights to provision and participation, often constrained by commercial and professional imperatives. This work posits that the availability of practical instruments and support mechanisms is crucial for facilitating the comprehensive embedding of children's rights by designers, thereby potentially mitigating the disparity between theoretical ideals and practical industry applications [Pothong et al. 2024b].

Similarly, Colvert et al. explore the integration of children's rights into digital product and service design, especially for play. Recognizing public doubt about digital play's benefits, Colvert et al. draws a comparison between traditional and digital play to develop "Playful by Design"principles. These principles are linked to the UN Convention on the Rights of the Child and guide designers to build digital spaces that prioritize safety and privacy while also fostering children's agency, creativity, and development through play. Additionally, this work also proposes a "Child Rights by Design"approach, suggesting that focusing on the right to play can be an initial step for wider ethical considerations in digital design [Colvert et al. 2024].

Lastly, Valença et al. scrutinize how major tech platforms manage children's data, concluding that current protections are often inadequate. They point out children's frequent online presence and lower awareness of privacy risks compared to adults, stressing platforms' obligation to prioritize children's rights and well-being. Valença et al. propose 19 legal requirements based on children's rights frameworks to help companies implement Privacy by Design specifically for young users. The results indicate the need to drive a fundamental change in how tech companies protect children, moving from reactive measures to proactive safeguarding [Valença et al. 2022].

3. Research Method

The study employed a structured methodological approach to develop an ethical design guide for EdTech platforms based on children's rights principles. Our research method consisted of six sequential phases designed to systematically identify, categorize, validate, and formalize ethical design practices.

The first phase was the **identification of ethical design practices**. It involved a comprehensive review of both formal academic literature and gray literature (including regulatory documents, industry reports, and technical guidelines) related to children's rights in digital environments, EdTech platforms, and ethical design principles. This review enabled us to extract potential practices that could form the foundation of our ethical design guide. We documented these initial practices in a structured spreadsheet, capturing their descriptions, sources, and preliminary categorizations.

Following the initial identification, we conducted an iterative **categorization process** to organize the practices into coherent thematic groups. Through collaborative analysis and discussion among the research team, we identified ten distinct categories encompassing various aspects of ethical design for EdTech platforms: *Governance and Policies*, *Data Protection and Privacy*, *Security and Technical Infrastructure*, *Child-Centered Design and Development*, *Inclusion and Accessibility*, *Pedagogical Practices and Educational Use*, *Artificial Intelligence and Emerging Technologies*, *Children's Rights and Autonomy*, *Commercial Aspects and Monetization*, *Transparency*. These categories were developed to ensure comprehensive coverage of key ethical considerations for children's interactions with educational technology.

In this phase, we performed a **regulatory alignment** by systematically analyzing each identified practice against relevant regulatory frameworks - including Brazil's General Data Protection Law (LGPD) [Brazil 2018], the National Council for the Rights of Children and Adolescents (CONANDA) Resolution Nº245 [National Council for the Rights of Children and Adolescents - CONANDA 2024], and international frameworks such as the United Nations Convention on the Rights of the Child (UNCRC) [Assembly e Directorate 1991]. This alignment process served to validate the practices and establish their legal foundations, ensuring that our recommendations were grounded in established regulatory principles rather than merely aspirational guidelines. Then, a **consolidation and refinement** aimed at ensuring the clarity and non-redundancy of our recommendations. We conducted a thorough review of the compiled practices, identifying and resolving duplications, overlaps, and inconsistencies. This consolidation process resulted in the final set of 78 distinct practices across the ten categories[5]. Each practice was refined to ensure precision in language and applicability to the EdTech context.

Finally, we conducted **actor identification**, i.e., for each practice, we mapped the relevant actors responsible for implementation or compliance. This step recognized that

[5] This wide set of practices is available at https://tinyurl.com/ihc2025-EDfEP

ethical design in EdTech ecosystems involves multiple stakeholders, including technology providers, educational institutions, government bodies, and legal guardians. By explicitly mapping responsibilities to specific actors, our guide acknowledges the distributed nature of ethical responsibility in digital educational environments.

4. Results

This section outlines key practices from our proposed Ethical Design Code, grounded in Privacy by Design principles. These practices address critical aspects of EdTech platform design and implementation, emphasizing the protection of children's rights and privacy. The categories encompass fundamental elements such as data privacy controls, data retention policies, purpose limitations, security measures, and governance structures. The following subsections present selected key practices, providing detailed explanations of their implementation requirements, regulatory bases, and supporting evidence from existing literature. Collectively, these practices form a framework that educational institutions can utilize to evaluate EdTech platforms and ensure they uphold children's rights within digital learning environments.

4.1. Children's Data Privacy and Control

Table 1. Detailed Attributes for Children's Data Privacy and Control

Practice 1	Children must have full control over their data and access to agile, effective, and confidential mechanisms for reporting abuse and violence in both digital and non-digital environments
Agent	EdTech
Applies To	Children
Complies With	LGPD and CONANDA Resolution Nº 245
Supporting Evidence	[Valença et al. 2024],[Batista et al. 2024]

To ethically design digital learning spaces, EdTech platforms must empower children with comprehensive control over their personal data and offer user-friendly reporting tools for abuse or violations. This establishes a crucial balance between data privacy and child safety.

Brazil's General Data Protection Law (LGPD), in Article 51, mandates that the national authority promote technical standards for personal data control. For EdTechs, this implies creating age-appropriate interfaces that enable children to understand and manage their privacy effectively. However, as Valença et al. highlight, many platforms employ manipulative designs that impede children's data control, reinforced the need for clear and child-friendly data management tools [Valença et al. 2024].

Furthermore, Brazil's Council for the Rights of Children and Adolescents (CONANDA) appoints in Resolution 245/2024 (Articles 21 and 30) requirements for easily accessible reporting tools built on simple language and transparent tracking mechanisms [National Council for the Rights of Children and Adolescents - CONANDA 2024]. EdTech companies must establish clear procedures for escalating reports to relevant authorities, including the National Human Rights Ombudsman, Child Protection Services, the Public Prosecutor's Office, the Public Defender's Office, and specialized law inforcement units when necessary. Batista et al. emphasize that these reporting tools must operate independently of parental controls, acknowledging that abuse can occur within families [Batista et al. 2024].

To achieve this, EdTech developers must consider children's developmental stages when designing both data controls and reporting systems. Key protective and empowering features include: age-appropriate privacy settings accompanied by clear and simple explanations; easily understandable reporting tools tailored to children's cognitive abilities; confidential reporting channels to prevent retaliation; visible and readily accessible help options integrated throughout the platform; and transparent information detailing how reports are handled and the associated timelines.

4.2. Data & Processing Ownership

Table 2. Detailed Attributes for Data & Processing Ownership

Practice 2	Identify and inform the respective data processor and data controller.
Agent	Schools
Applies To	EdTechs
Complies With	LGPD
Supporting Evidence	[Day 2021]

Data and Processing Ownership mandates that schools, as the primary entities responsible for children's data, must clearly identify and subsequently inform data subjects about the entities acting as data controllers and data processors. LGPD enforces the right of data subjects to have facilitated access to information regarding the identification and contact details of the controller, and the responsibilities of the agents involved in data processing. Thus, schools must ensure that both students and their legal guardians are made aware of who holds the role of controller (typically the school itself, determining the purposes and means of processing) and who acts as the processor (often the EdTech provider, processing data on behalf of the school).

Day et al. also highlights the complexities in determining these roles, noting that while schools are often data controllers for educational data, EdTech companies might act as processors under contract or even as independent controllers for their own purposes, such as product development [Day 2021]. Therefore, schools must meticulously define these roles in their contracts with EdTech providers. This proactive identification and communication are vital, as LGPD also stipulates that if a controller cannot immediately fulfill a data subject's request, it must clarify that it is not the processing agent and, where possible, identify the responsible agent. Moreover, LGPD also requires the public disclosure of the Data Protection Officer's (DPO) identity and contact information, reinforcing the principle of transparency in data governance.

4.3. Data Retention Policy

Data Retention Policy establishes requirements for the Government and Schools to implement a robust policy specifically designed for children's educational data, ensuring

Table 3. Detailed Attributes for Data Retention Policy

Practice 3	Implement a data retention policy for online services that limits the retention of children's data, specifically preventing educational data from being kept longer than required.
Agent	Federal Government and Schools
Applies To	EdTechs
Complies With	LGPD and CONANDA Resolution Nº 245
Supporting Evidence	[Day 2021, Singer 2023]

that such information is not stored beyond the necessary time-frame for its intended educational purpose. This practice addresses a significant gap identified in current governance frameworks where children's data processed through educational platforms is often retained indefinitely [Day 2021].

The LGPD mandates the termination of data processing when the purpose has been achieved or when the data is no longer necessary or relevant to the specific intended purpose [Brazil 2018]. Moreover, CONANDA Resolution Nº245 enforces the principle of collecting only the minimum necessary data and storing it only for the duration required to fulfill the purpose of its collection [National Council for the Rights of Children and Adolescents - CONANDA 2024].

For proper implementation, governmental agencies must establish clear guidelines specifying maximum retention periods for different categories of educational data. Schools must then develop explicit data retention schedules that define when children's data should be deleted, archived, or anonymized after fulfilling its educational purpose.

4.4. Data Integrity and Confidentiality

Table 4. Detailed Attributes for Data Integrity and Confidentiality

Practice 4	Implement appropriate security measures to safeguard the integrity and confidentiality of children's personal data
Agent	EdTechs and Schools
Applies To	Children's Data
Complies With	CONANDA Resolution Nº 245
Supporting Evidence	[Day 2021, Batista et al. 2024]

All entities responsible for handling children's personal data in digital environments, primarily EdTech providers and educational institutions, bear a critical responsibility to implement appropriate security measures. This necessitates the creation and ongoing management of comprehensive security protocols designed to ensure the data's integrity (accuracy and completeness) and confidentiality (restricted access) against a wide range of threats, including unauthorized access, processing, modification, disclosure, or destruction throughout the data's lifecycle.

Compliance regulations demand that these agents (EdTechs and schools) adopt a proactive, risk-informed strategy, implementing technical, physical, and administrative safeguards that are proportionate to the sensitivity of the data and the potential for harm. A key regulatory requirement is CONANDA via Resolution 245/2024, which, in Article 12, §2º, explicitly mandates "robust security measures."[National Council for the Rights of Children and Adolescents - CONANDA 2024]. This signifies that standard security practices are insufficient; measures must be demonstrably strong, current, and effective in mitigating identified risks. Consequently, agents must conduct regular risk assessments to identify vulnerabilities and potential threats within the often intricate data ecosystems associated with EdTech platforms, as highlighted by [Day 2021].

Effective risk mitigation involves the implementation of strong technical controls, such as data encryption (at rest and in transit), robust authentication and fine-grained access control mechanisms (e.g., role-based access), and the deployment of up-to-date network security tools like firewalls and anti-malware solutions. Secure software development lifecycles, regular vulnerability scanning, and the timely application of security patches are also critical technical components. Furthermore, the use of pseudonymization or anonymization techniques is encouraged where feasible to reduce inherent risks [Day 2021].

Complementing technical measures are essential administrative and organizational safeguards. This includes the development and enforcement of clear internal data security policies and well-defined incident response plans. Critically, regular and mandatory data protection training for all relevant personnel is required. Underlying these practices are the principles of Privacy by Design and by Default, which necessitate the integration of data protection, including security, from the initial stages of system design and operation, ensuring default settings prioritize privacy [Batista et al. 2024]. Additionally, the principle of Data Minimization, which restricts data collection and retention to what is strictly necessary for legitimate purposes (detailed in section 4.5), is fundamental. Finally, rigorous third-party management is essential, ensuring that vendors processing children's data adhere to equivalent security standards through thorough due diligence and legally binding agreements, thereby addressing potential accountability gaps [Day 2021, Valença et al. 2024].

4.5. Data Minimization

Table 5. Detailed Attributes for Data Minimization

Practice 5	Limit the collection of student personal data to that which is strictly necessary
Agent	Schools
Applies To	EdTechs
Complies With	CONANDA Resolution Nº 245
Supporting Evidence	[Valença et al. 2024, Day 2021, Singer 2023, Livingstone et al. 2021, 5Rights Foundation 2025]

Data Minimization refers to the principle that comprises rules for the collection of student personal data, which must be strictly limited to what is essential for a specified and legitimate purpose. This principle is directly supported by Article 12, paragraph 1, of the Brazilian CONANDA Resolution Nº 245, which stipulates that only the minimum amount of personal data necessary for the provision of a service should be gathered, and such data should be stored only for the period required to fulfill the objective of its collection [National Council for the Rights of Children and Adolescents - CONANDA 2024].

In the context of educational technologies (EdTechs), agents such as Schools and the Government bear the responsibility of ensuring compliance with this practice. This means that when EdTech platforms are utilized, these institutions must actively ensure that the data requested from students is demonstrably necessary for the educational service being provided, rigorously avoiding the collection of superfluous information. The implementation of data minimization by these agents is crucial for safeguarding children's privacy in digital learning environments, a concern underscored by various research and guidelines [Valença et al. 2024, Day 2021, Singer 2023, Livingstone et al. 2021, 5Rights Foundation 2025]. Therefore, adherence to data minimization requires a proactive approach from schools and governmental entities to scrutinize the data collection practices of EdTechs, thereby upholding the privacy rights of children as outlined in CONANDA Resolution Nº 245 [National Council for the Rights of Children and Adolescents - CONANDA 2024].

4.6. Data Use Limitation

Table 6. Detailed Attributes for Data Use Limitation

Practice 6	Data must not be used for any future purpose beyond the initially specified scope without explicit permission, adhering to the principle of purpose limitation.
Agent	EdTechs, Schools and Federal Government
Applies To	Children's Data
Complies With	LGPD and CONANDA Resolution Nº 245
Supporting Evidence	[Day 2021, Singer 2023, 5Rights Foundation 2025]

Children's data must not be utilized for any future purpose beyond the scope initially specified at the time of collection without obtaining new, explicit consent. This practice directly upholds the principle of purpose limitation, a cornerstone of data protection[Brazil 2018]. The responsibility for enforcing this limitation on children's data lies with EdTechs, Schools, and the Federal Government.

These agents must ensure that data collected for a specific educational activity is not subsequently repurposed for unrelated analytics, commercial profiling, or other uses not originally and clearly communicated. LGPD mandates that data processing must be carried out for legitimate, specific, and explicit purposes informed to the data subject, prohibiting subsequent processing in a manner incompatible with these original purposes.

CONANDA Resolution Nº 245 reinforces this, notably in Article 15, which prohibits the use of children's and adolescents' personal data for commercial ends, including behavioral profiling and market segmentation, unless explicit consent is provided for such new purposes. The necessity for clear, informed, and renewed consent for any new use of data is paramount [Day 2021, Singer 2023, 5Rights Foundation 2025]. Thus, EdTechs, schools, and governmental bodies must implement robust mechanisms to manage consent and ensure that children's data is used strictly in accordance with the purposes for which it was originally and transparently collected.

4.7. Data Purpose Definition

Table 7. Detailed Attributes for Data Purpose Definition

Practice 7	Explicitly define that the collection of children's data, particularly personal data, is solely for educational purposes and strictly prohibits commercial use.
Agent	EdTechs
Applies To	Children's data
Complies With	CONANDA Resolution Nº 245
Supporting Evidence	[Day 2021, Singer 2023]

Building upon the considerations in section 4.6, it is imperative that Educational Technology (EdTech) providers, even when data usage limitations are active, explicitly define that the collection of children's data, especially personal data, is exclusively for educational purposes. Any commercial use of this data must be strictly prohibited. This approach reinforces the ethical principle that data obtained from children should be used solely to support their learning and development, thereby safeguarding it from commercial exploitation [Day 2021]. Furthermore, this aligns with the mandates of CONANDA Resolution Nº 245, which underscores the necessity of restricting data use to prevent commercial exploitation through tracking and the creation of behavioral profiles derived from children's data. Consequently, EdTech entities must ensure their data collection and processing practices are precisely tailored to and focused on achieving educational objectives.

4.8. Public Purpose Data Sharing

Table 8. Detailed Attributes for Public Purpose Data Sharing

Practice 8	Sensitive data obtained from public sector bodies to educational software must only be shared when a clear public interest is demonstrated
Agent	Public Sector
Applies To	EdTechs
Complies With	LGPD
Supporting Evidence	[Day 2021]

Public Purpose Data Sharing dictates that sensitive data pertaining to children, when sourced from public sector bodies and provided to educational software (EdTechs), may only be shared if a distinct and demonstrable public interest validates such an action. This principle, primarily relevant to the Public Sector, is formulated to ensure adherence to data protection regulations, particularly the LGPD.

In accordance with this principle, the public sector agent is obligated to ensure that any dissemination of sensitive children's data collected through EdTech platforms strictly aligns with a clear public interest. As emphasized by the LGPD, the processing of public personal data must take into account the purpose, good faith, and the public interest that justified its initial availability [Brazil 2018].

Furthermore, a crucial element for the public sector in implementing this practice involves a comprehensive understanding and clear definition of the data's purpose before authorizing access, a concept further elaborated in section 4.7. This ensures that data sharing is not only justified by a significant public interest but also remains consistent with the original objectives for which the data was collected and processed.

4.9. Parental Control

Table 9. Detailed Attributes for Parental Control

Practice 9	Parental control features must be available on the platform
Agent	EdTechs
Applies To	Legal Guardians
Complies With	CONANDA Resolution Nº 245
Supporting Evidence	[Valença et al. 2024, Batista et al. 2024]

A cornerstone of digital platforms for children is parental control, which represents a critical safeguard mechanism ensuring appropriate oversight by legal guardians over minors' digital experiences. EdTechs are explicitly required to implement robust parental control features on their platforms, including mechanisms that limit the interaction of children and adolescents with unknown individuals.

The CONANDA Resolution Nº 245 reinforces this requirement, demanding that companies provide parental mediation mechanisms and actively recommend the participation of legal guardians. Additionally, the resolution establishes the right to protection against risks of contact and conduct by third parties that may jeopardize a child's safety. Offering parental moderation features on the platform, such as mechanisms that limit the interaction of children and adolescents with unknown persons, is a direct example of the application of these guidelines.

As highlighted by Valença et al. and Batista et al., platforms must develop parental control and mediation features within their software solutions to ensure children's privacy and security, while avoiding dark patterns that can frustrate or obscure these controls (e.g., obstruction or hidden settings or menus) [Valença et al. 2024, Batista et al. 2024].

4.10. Parental Consent Transparency

Parental Consent Transparency establishes a critical guideline for handling children's educational data. This practice designates the School as the primary agent responsible for its implementation.

The main goal of this practice is to restrict any type of sensitive data sharing collected through educational software by public sector bodies, such as schools, without proper parental consent. The LGPD establishes that the processing of personal data

Table 10. Detailed Attributes for Parental Consent Transparency

Practice 10	The collection, use, and sharing of children's data must be performed transparently and require informed consent from parents or guardians.
Agent	School
Applies To	Children's data and Legal guardians
Complies With	CONANDA Resolution Nº 245
Supporting Evidence	[Milkaite e Lievens 2020, Apps et al. 2024, Milkaite et al. 2021, Pangrazio e Bunn 2024, Singer 2023, 5Rights Foundation 2025]

of children must be carried out with specific and highlighted consent given by at least one parent or legal guardian. There are exceptions for the collection of data without consent, such as to contact parents or the legal guardian (used only once and without storage) or for their protection [Brazil 2018], but emphasizes that in no case may such data be transferred to a third party without consent. Alternatively, CONANDA Resolution Nº245 emphasizes the necessity of obtaining free, prior, specific, and informed consent from legal guardians for processing children's personal data, and whenever possible, from the child or adolescent, considering their maturity and understanding. Furthermore, Resolution Nº245 mandates that technology companies publish annual reports on their risk assessments concerning children's rights and interests, as well as independent audits evaluating their compliance with national legal frameworks [National Council for the Rights of Children and Adolescents - CONANDA 2024].

The school's responsibility extends to ensuring that any sharing of data is justifiable, documented, and communicated appropriately to the children and their legal guardians, respecting their right to privacy by default in all digital environments and services [National Council for the Rights of Children and Adolescents - CONANDA 2024, Milkaite e Lievens 2020, Apps et al. 2024, Milkaite et al. 2021, Pangrazio e Bunn 2024, Singer 2023, 5Rights Foundation 2025].

4.11. Records of Processing Activities

Table 11. Detailed Attributes for Records of Processing Activities

Practice 11	Maintain a comprehensive record of all categories of data processing activities
Agent	EdTechs
Applies To	Children and School data
Complies With	LGPD and CONANDA Resolution Nº245
Supporting Evidence	[Day 2021]

Maintain a comprehensive record of all categories of data processing activities delineates a crucial responsibility for EdTechs when handling Children's and School data. Thus, EdTechs must meticulously document all operations involving personal data.

The LGPD explicitly states that both controllers and operators maintain a record of the personal data processing operations they carry out, especially when based on legitimate interest [Brazil 2018]. Although CONANDA Resolution Nº 245 doesn't directly address the record of all categories, the resolution does establish obligations for companies to document, monitor, and report on their data processing activities involving children and adolescents, such as sharing data and evidence with academic researchers and civil society organizations studying the impact of digital environments on children [National Council for the Rights of Children and Adolescents - CONANDA 2024]. It also mandates that companies publish annual reports on Transparency, Risk assessments, and Independent audits.

Furthermore, the UK GDPR also underscores the importance of such record-keeping, where data processors have a legal duty to maintain a record of all categories of processing activities. This principle of accountability through comprehensive record-keeping is fundamental for ensuring that the processing of children's data is transparent, lawful, and serves their best interests [Day 2021].

4.12. Data Proportionality

Table 12. Detailed Attributes for Data Proportionality

Practice 12	Access to essential functionalities shall not be conditioned on the collection of excessive personal data.
Agent	EdTechs
Applies To	Children's and School data
Complies With	LGPD
Supporting Evidence	[5Rights Foundation 2025]

Data Proportionality establishes that access to any core functionalities of software platforms, particularly those provided by EdTechs, must not be contingent upon the collection of excessive personal data from children and schools. EdTechs must ensure compliance by limiting data collection to the absolute minimum necessary for the provision of their educational services (as detailed in Section 4.5). Therefore, Data Proportionality must not be dictated by business needs but by the level of risk to the child. If a system cannot operate without collecting excessive data in a way that conforms with protective codes, its application must be narrowed, or it should not be operated at all, especially when it impacts children [5Rights Foundation 2025].

While the LGPD doesn't directly address this practice, it empowers data subjects to request the anonymization, blocking, or deletion of unnecessary or excessive data. Thus, refusing to provide excessive data should not disproportionately obstruct access to a platform's core educational functionalities.

5. Discussion

The extensive adoption of EdTech platforms globally, such as Google Classroom, has ignited substantial worries regarding the privacy and safety of children's data. This is primarily due to the increasingly data-intensive nature of these platforms, which capture a wide array of personally identifiable information from children as they engage in learning activities [Hooper et al. 2022]. Although Google publicly states that data from K-12 users within its core educational services[6] is not used for advertising and that personal information is never sold to third parties for targeted ads, Google Classroom's data collection and processing methods still raise concerns.

Platform policies permit the collection of various types of data from children, which can be combined to form comprehensive profiles detailing identity, location, preferences, and capabilities [Livingstone et al. 2024b]. For example, when teachers share links on the platform, whether to external services like Vimeo or Google's own services like YouTube, children may encounter privacy protection levels that are less stringent than what should be expected for the main educational service [Pothong et al. 2024a]. These issues are consistent with proposed practices 4.7 and 4.12, which underscore the need for EdTech companies to have built-in privacy requirements from the outset. Furthermore, it remains unclear whether parents and guardians have any meaningful control over the data collected from children within the platform, a point reinforced by practice 4.12.

This situation poses a significant risk that companies like Google might process this data beyond the explicit directives of schools, potentially utilizing this data to develop new products or other commercial ventures. This concern is highlighted by practices 4.9 and 4.10, which shine a light on potential infringements on data minimization and purpose limitation principles, further outlined in practice 4.5. Moreover, these data processing procedures are frequently intricate and lack transparency, making it challenging for schools, who are designated as "data controllers", to fully grasp how data is managed, when and how it is shared, and the potential ramifications.

Practices 4.1 and 4.2 aim to hold companies responsible for their privacy safeguards and their lack of transparency regarding data handling. This lack of clarity impedes schools from effectively assessing data protection risks in a complex digital landscape dominated by large tech corporations, emphasizing the need for practice 4.8 to shield children's personal data from opaque corporate practices. Additionally, practices 4.5 and 4.10 call for further measures to ensure clear communication about data retention periods and the security protocols in place to protect the data.

The very design of Google Classroom also contributes to data protection risks by blurring the distinction between "core" services intended to respect privacy and "additional" services with commercial implications. Research indicates that users can easily move between these two categories, and investigations have revealed that accessing external content linked within Classroom can expose children to numerous third-party trackers used for advertising and analytics [Livingstone et al. 2024b].

Here again, practice 4.9 aims to determine the boundaries for all types of data usage, complemented by practice 4.10 to specify the purpose of data collection and practice 4.7, ensuring that parents and guardians are fully informed about the child data retained by these companies. This extensive flow of data into the global ecosystem leaves children's information susceptible to breaches, commercial exploitation, and long-term privacy risks, potentially infringing upon a child's right to freedom

[6] Google Workspace for Education Terms of Service | `https://workspace.google.com/terms/education_terms/`

from such exploitation (Article 32, UNCRC) and impacting various other child rights [Livingstone et al. 2024b][Pothong et al. 2024a]. These concerns require close monitoring through practice 4.4 in order to hold data controllers are accountable for any potential mishandling of children's data.

6. Conclusion

In terms of **contribution**, we believe the analysis of ethical design practices for EdTech platforms reveals critical gaps between current implementations and the desired Ethical Design for digital platforms. The twelve detailed practices in this research provide a comprehensive guideline that addresses data privacy, purpose limitation, security, and parental control, grounded in both legal frameworks and ethical design principles. In addition, our analysis of Google Classroom as a case study shows that even as a widely adopted platform, it falls short of these principles of Ethical Design, especially regarding transparency of data processing, purpose limitation, and the clear relations between educational and commercial interests. Moreover, the complexity of data flows highlights the unequal balance between Big Tech companies and educational institutions. Therefore, enforcing that vulnerable groups, such as children and local schools, overcome commercial interests prioritizing children's wellbeing, development, and rights [de Oliveira et al. 2024]

The proposed ethical design guide represents a significant step toward rectifying these issues by providing concrete, actionable practices that distribute responsibilities appropriately among EdTechs, schools, and governmental bodies. By implementing these practices, stakeholders can better protect children's data and rights while still benefiting from the educational advantages that technology offers, grounded by established regulatory principles rather than merely aspirational guidelines.

As **future work**, we intend to expand our ethical design code to incorporate additional dimensions, such as children's well-being, equity, and diversity. This enhanced version will provide more fine-grained recommendations for designers, including practical guidance and illustrative examples to support the implementation of the code. Furthermore, we aim to develop a standardized assessment tool that can be adopted by educational institutions - such as schools and local governments - to evaluate EdTech platforms. This includes benchmarking the tool's adoption and effectiveness across widely used educational technologies to promote alignment with ethical design principles.

7. Human Aspects

This research did not involve human participants. Therefore, no specific ethical approvals or informed consent procedures were required.

8. Acknowledgments

Please note that generative AI tools were used in certain sections of this paper to assist with grammar and spelling corrections.

Referências

5Rights Foundation (2025). Children & ai design code: A protocol for the development and use of ai systems that impact children. Technical report, 5Rights Foundation.

Apps, T., Beckman, K., e Ng, R. (2024). Datafied by default: Examining the intersect between children's digital rights and education.

Assembly, U. N. G. e Directorate, C. H. R. (1991). *Convention on the Rights of the Child*. Human Rights Directorate.

Batista, L., Pereira, M. C. M., Canto, M., Amaral, P., Neto, P. S., Saraiva, R. L., e Valois, R. (2024). *Termômetro do acesso adequado à idade: endereçando o acesso apropriado para crianças e adolescentes em plataformas digitais*. IP.Rec.

Brazil (2018). Lei nº 13.709, de 14 de agosto de 2018 - lei geral de proteção de dados pessoais (lgpd). Published in the Diário Oficial da União on August 15, 2018.

Brignull, H., Leiser, M., Santos, C., e Doshi, K. (2023). Deceptive patterns – user interfaces designed to trick you.

Colvert, A., Pothong, K., e Livingstone, S. (2024). Playful by design: Embedding children's rights into the digital world. *Games Research and Practice*.

Day, E. (2021). Governance of data for children's learning in uk state schools. Technical report, London School of Economics and Political Science, LSE Library.

de Oliveira, L. C., Amaral, M. A. a., Bim, S. A., Valença, G., Almeida, L. D. A., Salgado, L. C. d. C., Gasparini, I., e da Silva, C. B. R. (2024). Grandihc-br 2025-2035 - gc3: Plurality and decoloniality in hci. In *Proceedings of the XXIII Brazilian Symposium on Human Factors in Computing Systems*, IHC '24. Association for Computing Machinery.

eSafety Commissioner (2025). Behind the screen: The reality of age assurance and social media access for young australians. Technical report, Australian Government.

Fansher, M., Chivukula, S. S., e Gray, C. M. (2018). #darkpatterns: Ux practitioner conversations about ethical design. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI EA '18, page 1–6, New York, NY, USA. Association for Computing Machinery.

Greenberg, S., Boring, S., Vermeulen, J., e Dostal, J. (2014). Dark patterns in proxemic interactions. *Proceedings of the 2014 conference on Designing interactive systems - DIS '14*.

Hooper, L., Livingstone, S., e Pothong, K. (2022). Problems with data governance in uk schools: the cases of google classroom and classdojo. Technical report, London School of Economics and Political Science, LSE Library.

Kollmer, T. e Eckhardt, A. (2022). Dark patterns. *Business & Information Systems Engineering*, 65.

Lacey, C. e Caudwell, C. (2019). Cuteness as a 'dark pattern' in home robots. *2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*.

Livingstone, S., Atabey, A., e Pothong, K. (2021). Addressing the problems and realising the benefits of processing children's education data: Report on an expert roundtable. Technical report, London School of Economics and Political Science, LSE Library.

Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., e Kidron, B. (2024a). The best interests of the child in the digital environment. Technical report, London School of Economics and Political Science, LSE Library.

Livingstone, S. e Pothong, K. (2023). Child rights by design: Guidance for innovators of digital products and services used by children. *Digital Futures Commission*.

Livingstone, S., Pothong, K., Atabey, A., Hooper, L., e Day, E. (2024b). The googlization of the classroom: Is the uk in protecting children's data and rights? *Computers and Education Open*, 7:100195–100195.

Livingstone, S. e Stoilova, M. (2021). *The 4Cs: Classifying Online Risk to Children*. CO:RE Short Report Series on Key Topics. Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI), Hamburg.

Lundgren, B. (2023). In defense of ethical guidelines. *AI and Ethics*, 3(3):1013–1020.

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., e Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3:1–32.

Michael, K. (2024). Mitigating risk and ensuring human flourishing using design standards: Ieee 2089-2021 an age appropriate digital services framework for children. *IEEE Transactions on Technology and Society*, pages 1–13.

Milkaite, I., De Wolf, R., Lievens, E., De Leyn, T., e Martens, M. (2021). Children's reflections on privacy and the protection of their personal data: A child-centric approach to data protection information formats. *Children and Youth Services Review*, 129:106170.

Milkaite, I. e Lievens, E. (2020). Child-friendly transparency of data processing in the eu: from legal requirements to platform policies. *Journal of Children and Media*, 14(1):5–21.

National Council for the Rights of Children and Adolescents - CONANDA (2024). Resolução nº 245, de 5 de abril de 2024. Published in the Diário Oficial da União on April 5, 2024.

Núcleo de Informação e Coordenação do Ponto BR (2024). Pesquisa sobre o uso da internet por crianças e adolescentes no brasil: Tic kids online brasil, ano 2024. Disponível em: `http://cetic.br/pt/arquivos/kidsonline/2024/criancas`. Acessado em: 25 de agosto de 2025.

Pangrazio, L. e Bunn, A. (2024). Assessing the privacy of digital products in australian schools: Protecting the digital rights of children and young people. *Computers and Education Open*, 6:100187.

Pothong, K., Hooper, L., Livingstone, S., Atabey, A., e Day, E. (2024a). The 'googlisation' of the classroom: How does the protection of children's personal data fare? *AoIR Selected Papers of Internet Research*.

Pothong, K., Livingstone, S., Colvert, A., e Pschetz, L. (2024b). Applying children's rights to digital products: Exploring competing priorities in design. In *Proceedings of the 23rd Annual ACM Interaction Design and Children Conference*, IDC '24, page 93–104, New York, NY, USA. Association for Computing Machinery.

Sánchez Chamorro, L., Bongard-Blanchy, K., e Koenig, V. (2023). Ethical tensions in ux design practice: Exploring the fine line between persuasion and manipulation in online interfaces. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, DIS '23, page 2408–2422, New York, NY, USA. Association for Computing Machinery.

Singer, N. (2023). U.s. regulators propose new online privacy safeguards for children. *The New York Times*.

Tilsner, M., Fiech, A., Zhan, G., e Specht, T. (2011). Patterns for service composition. *CiteSeer X (The Pennsylvania State University)*, pages 133–137.

Valença, G., Sarinho, M. W., Polito, V., e Lins, F. (2022). Do platforms care about your child's data? a proposal of legal requirements for children's privacy and protection. In *WER*.

Valença, G., Silva, J. V., Rocha, B., e Cortiz, D. (2024). Children's rights not deceptive patterns by design: a requirements perspective. In *Proceedings of the XXIII Brazilian Symposium on Human Factors in Computing Systems*, pages 1–11.

Zagal, J. P., Björk, S., e Lewis, C. (2013). Dark patterns in the design of games. *Foundations of Digital Games*, pages 39–46.