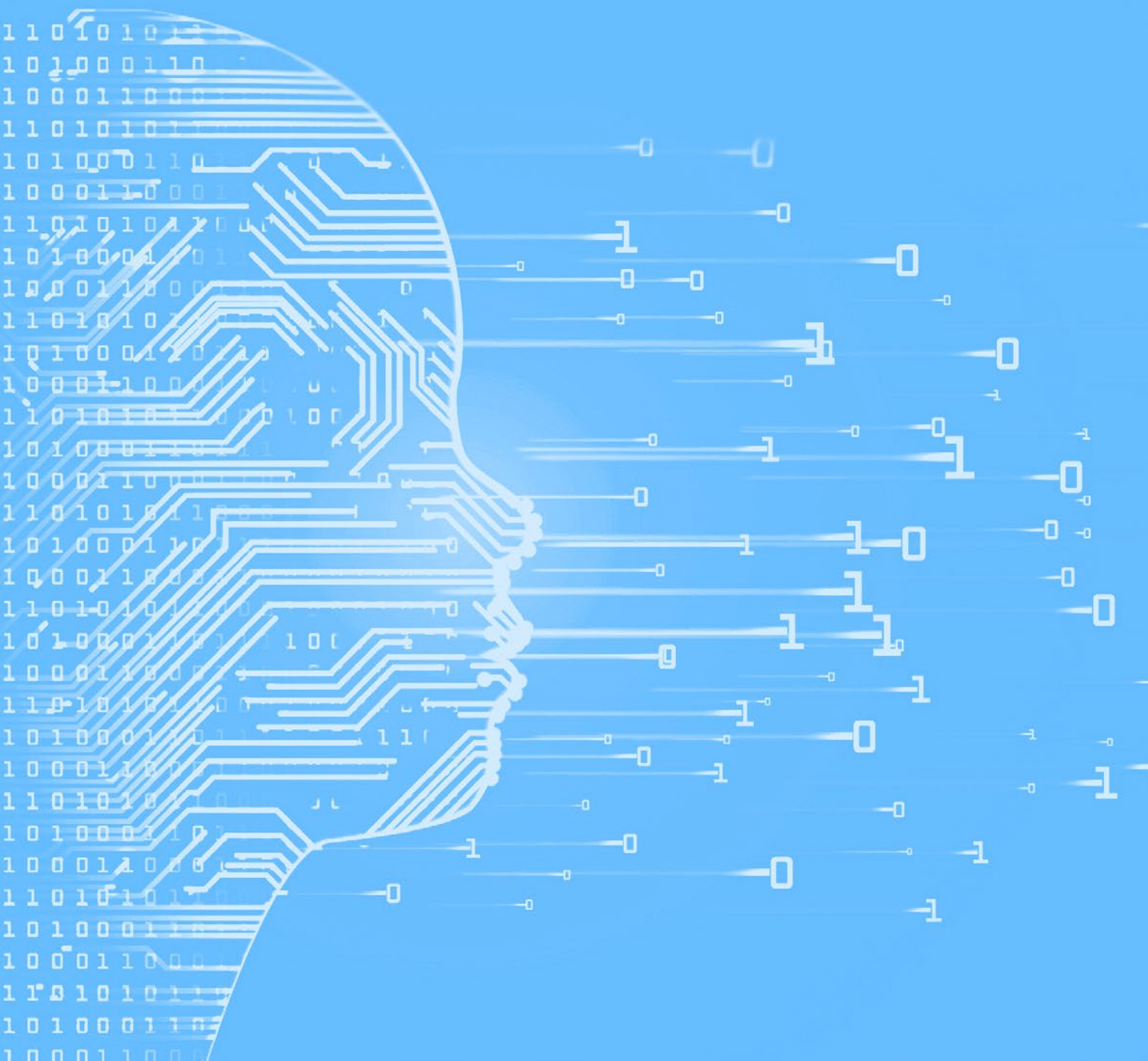
WORLD ECONOMIC FORUM

Artificial Intelligence for Children

TOOLKIT

MARCH 2022



Images: Getty Images

Contents

Introduction

This toolkit is designed to help companies develop trustworthy artificial intelligence for children and youth.

For the first time in history, a generation of children is growing up in a world shaped by artificial intelligence (AI). AI is a set of powerful algorithms designed to collect and interpret data to make predictions based on patterns found in the data.

Children and youth are surrounded by AI in many of the products they use in their daily lives, from social media to education technology, video games, smart toys and speakers. AI determines the videos children watch online, their curriculum as they learn, and the way they play and interact with others.

This toolkit, produced by a diverse team of youth, technologists, academics and business leaders, is designed to help companies develop trustworthy artificial intelligence (AI) for children and youth and to help parents, guardians, children and youth responsibly buy and safely use AI products.

AI can be used to educate and empower children and youth and have a positive impact on society. But children and youth can be especially vulnerable to the potential risks posed by AI, including bias, cybersecurity and lack of accessibility. AI must be designed inclusively to respect the rights of the child user. Child-centric design can protect children and youth from the potential risks posed by the technology.

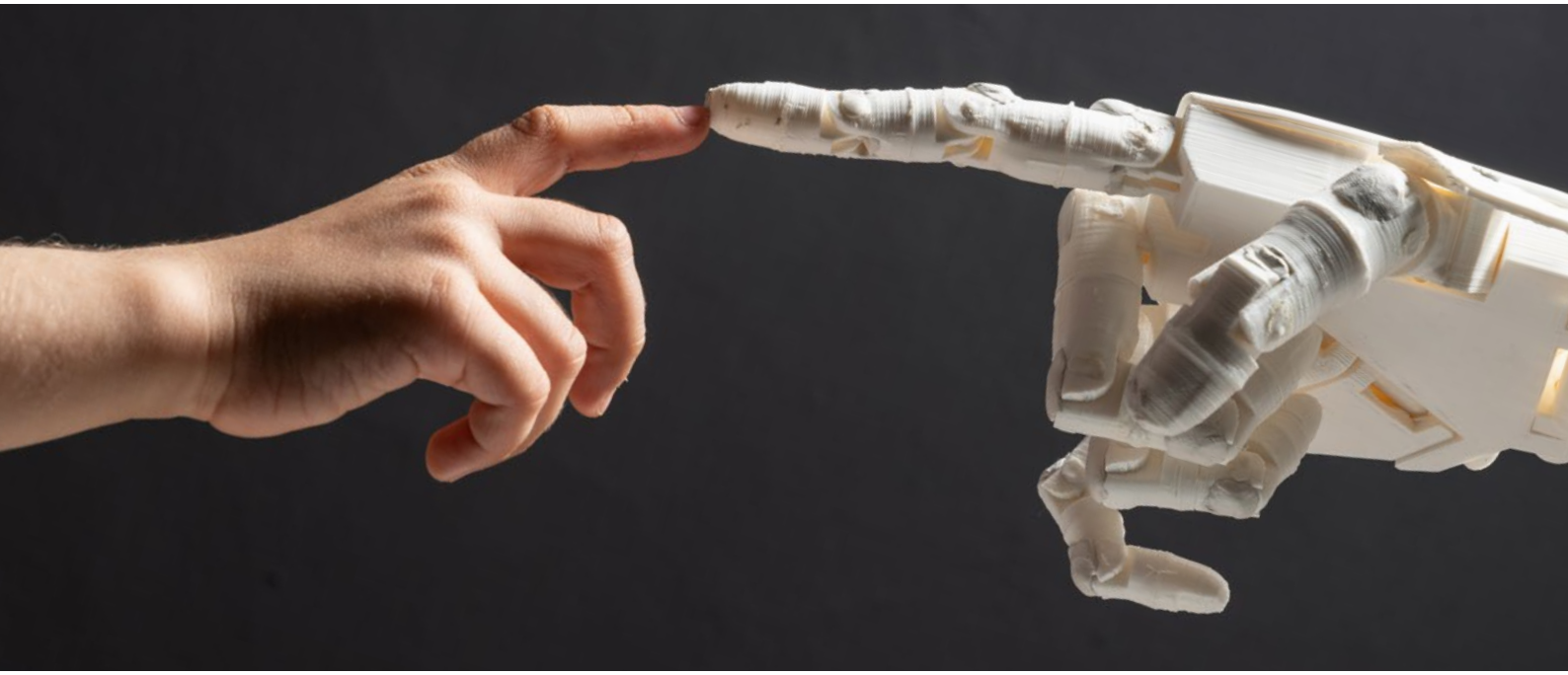
AI technology must be created so that it is both innovative and responsible. Responsible AI is safe, ethical, transparent, fair, accessible and inclusive. Designing responsible and trusted AI is good for consumers, businesses and society. Parents, guardians and adults all have the responsibility to carefully select ethically designed AI products and help children use them safely.

What is at stake? AI will determine the future of play, childhood, education and societies. Children and youth represent the future, so everything must be done to support them to use AI responsibly and address the challenges of the future.

This toolkit aims to help responsibly design, consume and use AI. It is designed to help companies, designers, parents, guardians, children and youth make sure that AI respects the rights of children and has a positive impact in their lives.

Putting children and youth FIRST checklist

- [ ] **F**air
- [ ] **I**nclusive
- [ ] **R**esponsible
- [ ] **S**afe
- [ ] **T**ransparent



Who are you?

A corporate decision-maker, member of a product team or a parent or guardian?

Corporate users

The checklist for **C-suite executives** and guidelines for product teams contain actionable frameworks and real-world guidance to help your company design innovative and responsible AI for children and youth. By using these guidelines, you can lead as a trusted company that delights your child users.

Companies should keep in mind that children often use AI products that were not designed specifically for them. It's sometimes difficult to predict what products might later be used by children or youth. As a result, you should carefully consider whether children or youth might be users of the technology you're developing. If they are, you should carefully consider how to help increase the benefits and mitigate potential risks posed by the technology for children and youth.

The C-suite is responsible for setting the culture around responsible AI and strategy for and investment in AI products. The checklist is designed to help executives learn more about the benefits and risks of AI for children and youth so you can better lead, innovate and grow.

Read more about the C-suite checklist.

Product teams design, develop and deploy the AI technology that children and youth will use. Responsible design starts with product teams and continues to be their ongoing responsibility. The guidelines are designed for engineers, developers, product managers and other members of the product team to use throughout the product life cycle.

> **Companies should keep in mind that children often use AI products that were not designed specifically for them.**

AI labelling system

The AI labelling system is designed to be included in all AI products on their physical packaging and online accessible through a QR code. Like nutritional information on food packaging, the labelling system is designed to concisely tell consumers – including parents and guardians, as well as children and youth – how it works and the options available to the users. All companies are encouraged to adopt this tool to help create greater trust and transparency with the purchasers and child users of their products.

Learn about the AI labelling system

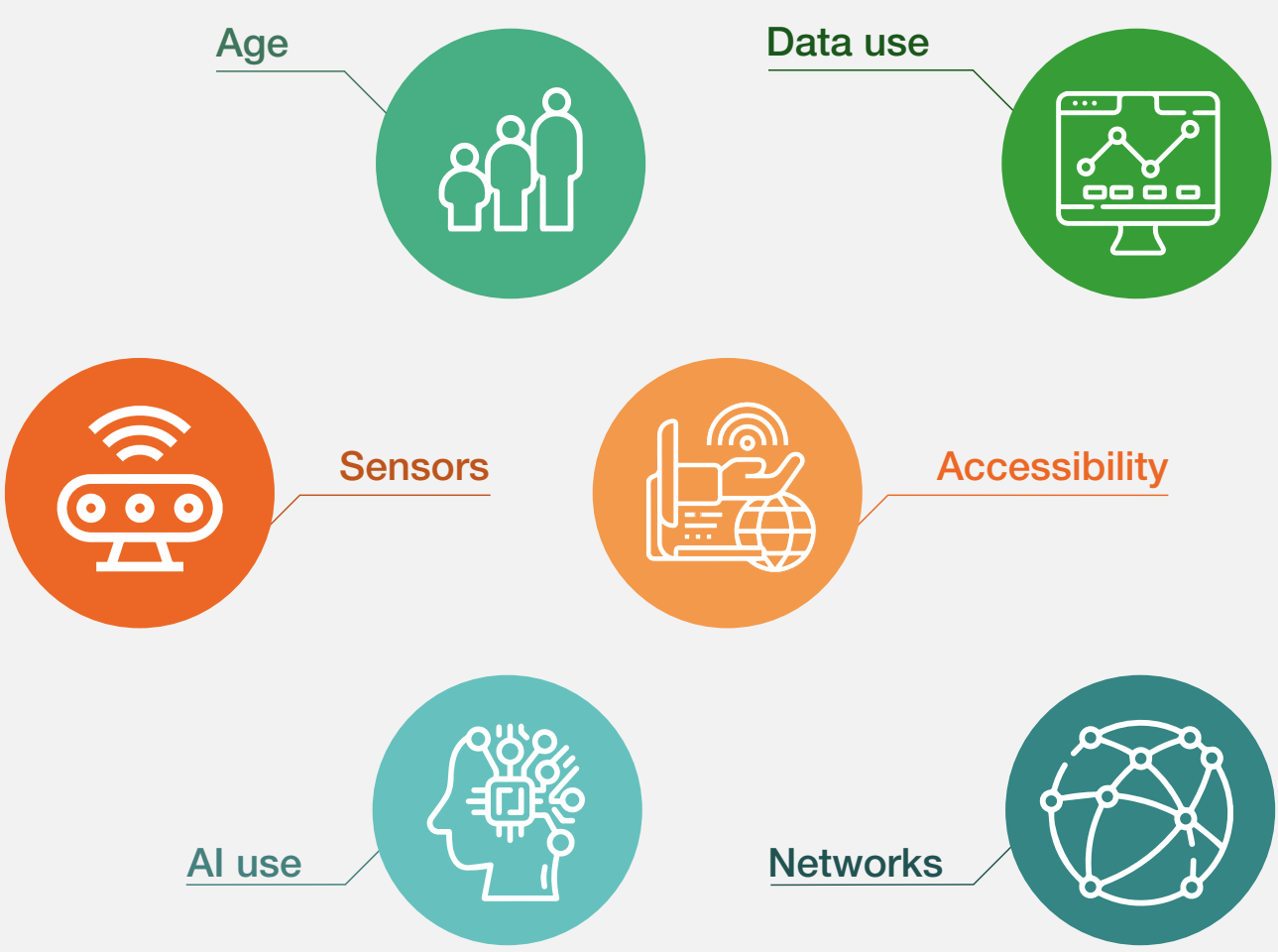
Consumers: Parents and guardians

Parents and guardians decide which AI-powered technologies to buy for their children. By educating yourselves and better understanding the benefits and risks posed by the technology, you can make deliberate and informed decisions that can protect your children and be sure AI has a positive impact on their lives.

Learn more about the Guide for parents and guardians

The tool for parents and guardians is designed based on the AI labelling system (Figure 1) to understand these six important categories of AI.

FIGURE 1 **AI labelling system**



Source: World Economic Forum

1

C-suite and corporate decision-makers' checklist

Actionable frameworks and real-world guidance help companies design innovative and responsible AI for children and youth.

This checklist is for C-suite executives of companies that provide products and services incorporating artificial intelligence (AI) intended for use by children and youth. Many companies use AI to differentiate their brands and their products by incorporating it into toys, interactive games, extended reality applications, social media, streaming platforms and educational products. With little more than a patchwork of regulations to guide them, organizations must navigate a sea of privacy and ethics concerns related to data capture and the training and use of AI models. Executive leaders must strike a balance between realizing the potential of AI and helping reduce the risk of harm to children and youth and, ultimately, their brand. Building on a foundation established in the World Economic Forum "Empowering AI Leadership: AI C-Suite Toolkit", the checklist is intended to help C-suite executives and other corporate decision-makers reflect upon and act to create and support responsible AI for this vulnerable population.

Trusted and responsible AI for children and youth: A checklist for executives

Attracted by the extraordinary opportunity to innovate with AI, companies are moving at a record pace to incorporate AI into toys, broadcast and social media, smart speakers, education technology, virtual worlds and more.

AI ranges in complexity and impact from simple recommendation and customization engines to deeply immersive experiences that imitate and simulate human behaviour, emotions and interactions. Implemented thoughtfully, these systems can delight, teach and evoke interaction with their young users, enabling them to grow and develop at their own pace and according to their learning styles. But implemented without careful forethought and the guidance of child development experts and ethicists, AI can hinder development and infringe on the rights of vulnerable users.

With the checklist, leaders can learn how even companies that mean well overlook potential issues and how to mitigate the risks associated with AI adoption. Executives should aspire to the highest possible ethical and social standards regarding child development, suitability for purpose, non-bias, accessibility and privacy. Doing so provides tremendous potential beyond the opportunity to do good. It can elevate your brand and enable you to position your company as a trustworthy steward of sought-after products and services to your primary buyers: parents, grandparents, teachers, educators and other care providers.

Where companies can fall short

Executive leaders should create a culture of responsibility backed by resources that enable responsible AI from design to end-of-product use and beyond.

Given the acceleration of AI adoption and a lag in broadly accepted standards and guidance, leaders might be caught off guard. What are the riskiest behaviours that your teams should avoid?

- **Not disclosing how AI is used**: Companies that think buyers may object to AI may conceal or downplay its use. Be transparent about the use of AI and why you are using it.
- **Amplifying and perpetuating bias**: AI modelling can contain inaccuracies and oversimplifications that lead to inaccessibility and bias against marginalized groups, such as disabled communities and users from different cultural and socio-economic backgrounds.
- **Skipping user-focused validation**: Bypassing user and expert validation of suitability for purpose during design and prototyping stages can diminish the potential value of AI and cause harm.
- **Leaving privacy and security gaps**: Data security, privacy and consent to collect and use data are complicated due to cybersecurity threats and a patchwork of regulations that vary geographically. These concerns reach past the useful life of a product: For minors, parents provide consent, but their children may claim their right for their data to be forgotten as they get older.

With these potential stumbling blocks in mind, what steps can corporate leaders take to protect and enhance their brand while leveraging the remarkable potential of AI?

Actions

Executive leaders should create a culture of responsibility backed by resources that enable responsible AI from design to end-of-product use and beyond. These steps are recommended:

1. **Know the legal duties and regulatory constraints**:
   Leverage existing guidance, such as the Institute of Electrical and Electronics Engineers' (IEEE) Code of Ethics,[1] UNICEF's Policy Guidance on AI for Children[2] and World Economic Forum guidance,[3] as well as the guidance contained in this toolkit and guidelines for the product team, AI labelling system, and resources for parents and guardians and children and youth. Commit to internal and, if possible, external AI oversight. Report compliance and leadership measures publicly and in simple language so buyers can understand.

2. **Build a diverse and capable team:**
   Include ethicists, researchers, privacy specialists, educators, child development experts, psychologists, user-experience (UX) designers and data scientists. Collaborate with non-profit organizations and educational and research institutions for more expertise.

3. **Train your team and provide resources for success with this checklist:**
   Educate team members about the importance of responsible and trustworthy AI and provide them access to the skills, tools and time they need to execute your vision. Have open dialogue about unintended consequences, possible worst-case scenarios, and the reasons for ensuring your teams are considering the five AI characteristics critical to putting children and youth FIRST (Figure 2).

   For more information, refer to the product team guidelines, which offers detailed guidance on the five areas.

4. **Offer expertise to inform development of regulations, standards and guidance:**
   Contribute to public forums on how AI is being used in your products or services. Share your experience in proposing guidance and requirements.

5. **Welcome principled efforts to label products and services:**
   These should be done according to the potential impact of AI on users. Endorse and participate in activities to develop labelling and rating standards. Label your offerings to help consumers make informed choices based on recommendations about, for example, user age, accessibility factors and whether a camera and microphone are being used. For additional information about labelling recommendations, see the AI labelling system.

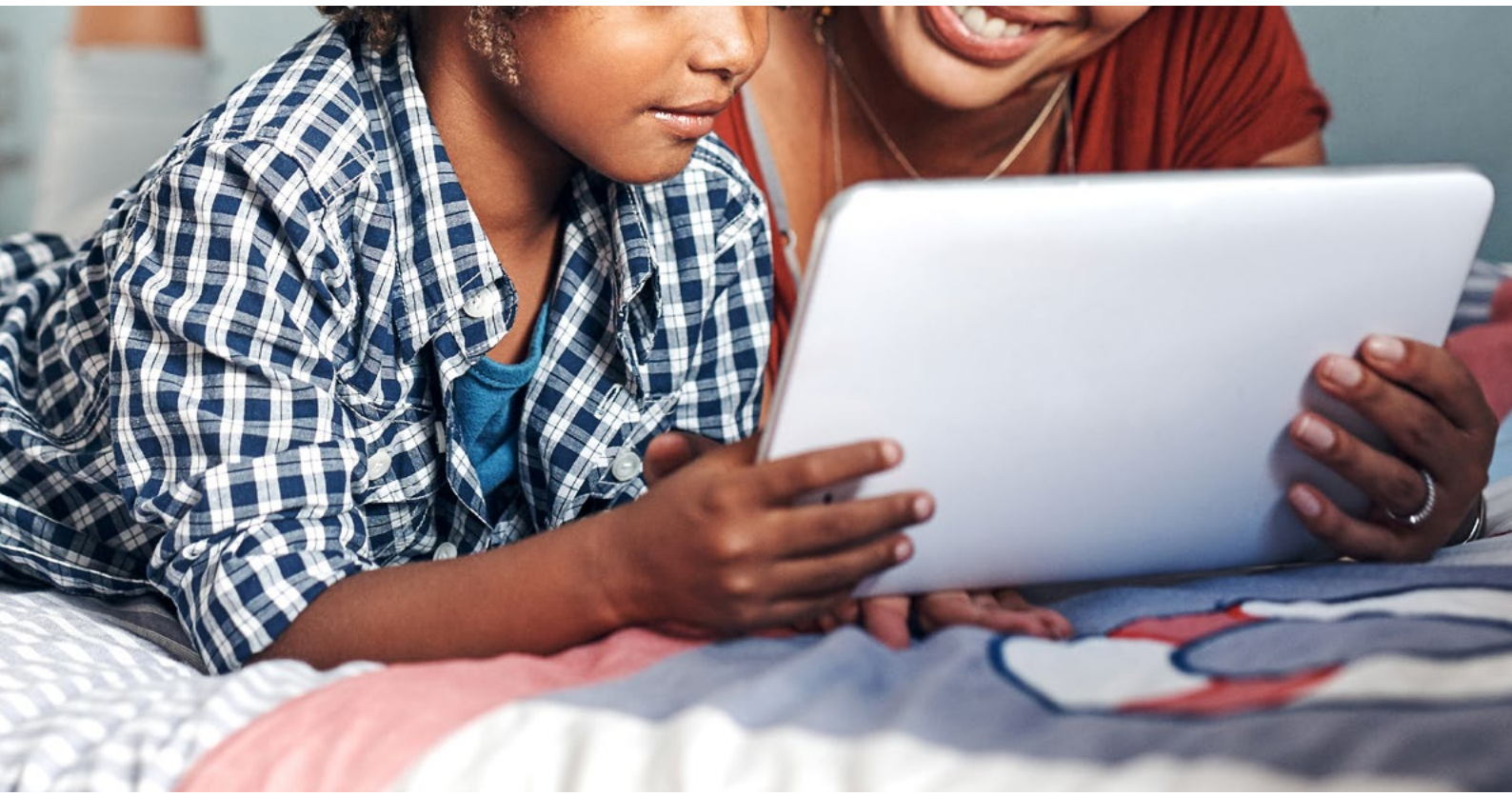
FIGURE 2 **Putting children and youth FIRST checklist**

Fair	Company culture and processes address ethics and bias concerns regarding how AI models are developed by people and the impact of AI models in use.
Inclusive	AI models interact equitably with users from different cultures and with different abilities; product testing includes diverse users.
Responsible	Offerings reflect the latest learning science to enable healthy cognitive, social, emotional and/or physical development.
Safe	The technology protects and secures user and purchaser data, and the company discloses how it collects and uses data and protects data privacy; users may opt out at any time and have their data removed or erased.
Transparent	The company explains in non-technical terms to buyers and users why AI is used, how it works and how its decisions can be explained. The company also admits AI's limitations and potential risks and welcomes oversight and audits.

Source: World Economic Forum

The rewards of leading

When you deliver responsible AI-based offerings and engage in the development of standards, you can do much more than just affect your bottom line. You help young users grow into the best versions of themselves – a generation empowered by AI.



References

- Benjamin, Ruha, *Race after Technology: Abolitionist Tools for the New Jim Code*, Polity Books, 2019, https://academic.oup.com/sf/article-abstract/98/4/1/5681679?redirectedFrom=fulltext
- Coeckelbergh, Mark, *AI Ethics*, MIT Press, 2020, https://mitpress.mit.edu/books/ai-ethics
- Dubber, Markus D., Frank Pasquale and Sunit Das (eds), *The Oxford Handbook of Ethics of AI*, Oxford University Press, 2020, https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780190067397.001.0001/oxfordhb-9780190067397
- O'Neil, Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown Publishing Group, 2016, http://www.governance40.com/wp-content/uploads/2019/03/Weapons-of-Math-Destruction-Cathy-ONeil.pdf
- Russell, Stuart, *Human Compatible: Artificial Intelligence and the Problem of Control*, Penguin Publishing Group, 2019, https://books.google.ch/books/about/Human_Compatible.html?id=8vm0DwAAQBAJ&redir_esc=y
- United Nations, "Young people help draw up UN digital protection recommendations", UN News, 24 March 2021, https://news.un.org/en/story/2021/03/1088182

2

Product team guidelines

Responsible design starts with product teams and continues to be their ongoing responsibility throughout the product life cycle.

Introduction

Why?

Product teams design, develop and deploy the AI technology that children and youth will use. Responsible design starts with product teams and continues to be your ongoing responsibility throughout the product life cycle. These guidelines are designed to help you develop responsible AI products for children and youth.

Who?

The entire product team: developers, programme managers, technical writers, product owners, software architects, UX designers, marketing managers and anyone else with a hand in product development.

How?

Dive into the five categories of "Putting children and youth FIRST" – Fair, Inclusive, Responsible, Safe and Transparent (Figure 3). Each theme is also organized into three sections: goals, greatest potential for harm, and mitigate risks. Use these categories and resources as a starting point. Responsible AI is a journey, and you'll want to form a diverse and dynamic team as you develop AI for children and youth.

FIGURE 3 **Putting children and youth FIRST**

Fair	Ethics, bias and liability
Inclusive	Accessibility, neuro-differences and feedback from kids
Responsible	Age- and developmental-stage-appropriate, reflects the latest learning science and is designed with kids in mind
Safe	Does no harm; cybersecurity and addiction mitigation
Transparent	Can explain how the AI works and what it is being used for to a novice or lay audience

Source: World Economic Forum

Foundational principles

The United Nations Convention on the Rights of the Child lays out numerous principles for protecting the rights, dignity, autonomy and safety of children. But the first principle under Article 3 guides many of the others:

"In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."[4]

> The best place to start is with a simple question: "Does the system I'm building have the best interests of children in mind?"

The best place to start is with a simple question: "**Does the system I'm building have the best interests of children in mind?**" Perhaps the answer is not "no", but "I'm not sure". And what if it is an emphatic "yes!"? No matter the answer, it is important to consider whether the positive impact can be clearly articulated and establish strategies for determining whether or not your system is having this intended impact. The goal of these guidelines is to help you identify the risks and uncover potential blind spots as a product is envisioned, built, tested and deployed.

Human-centred design is the act of starting first with the person for whom a product is being built. In that way, it is possible to prioritize the needs, desires and scenarios of use *over* the capabilities of the technology. Building products for children entails going a step further and taking a child-centred design approach.[5] In doing so, you will take more responsibility for the psycho-social development stage of your customers, the risks they may encounter with your technology, and your role in limiting harm. Doing so can help you ask the right questions about not only the desirability of your product, but also the fitness and safety of it.

These guidelines are not just for product teams building with children and youth in mind. They are relevant to products that children and youth **might** use. Social, media, gaming and even productivity platforms are all highly likely to be used by children and youth, independent of the expressed or implied target age.[6] Because of this, the hope is that these guidelines are applied across more than just the narrowly defined market of smart toys for children and youth.

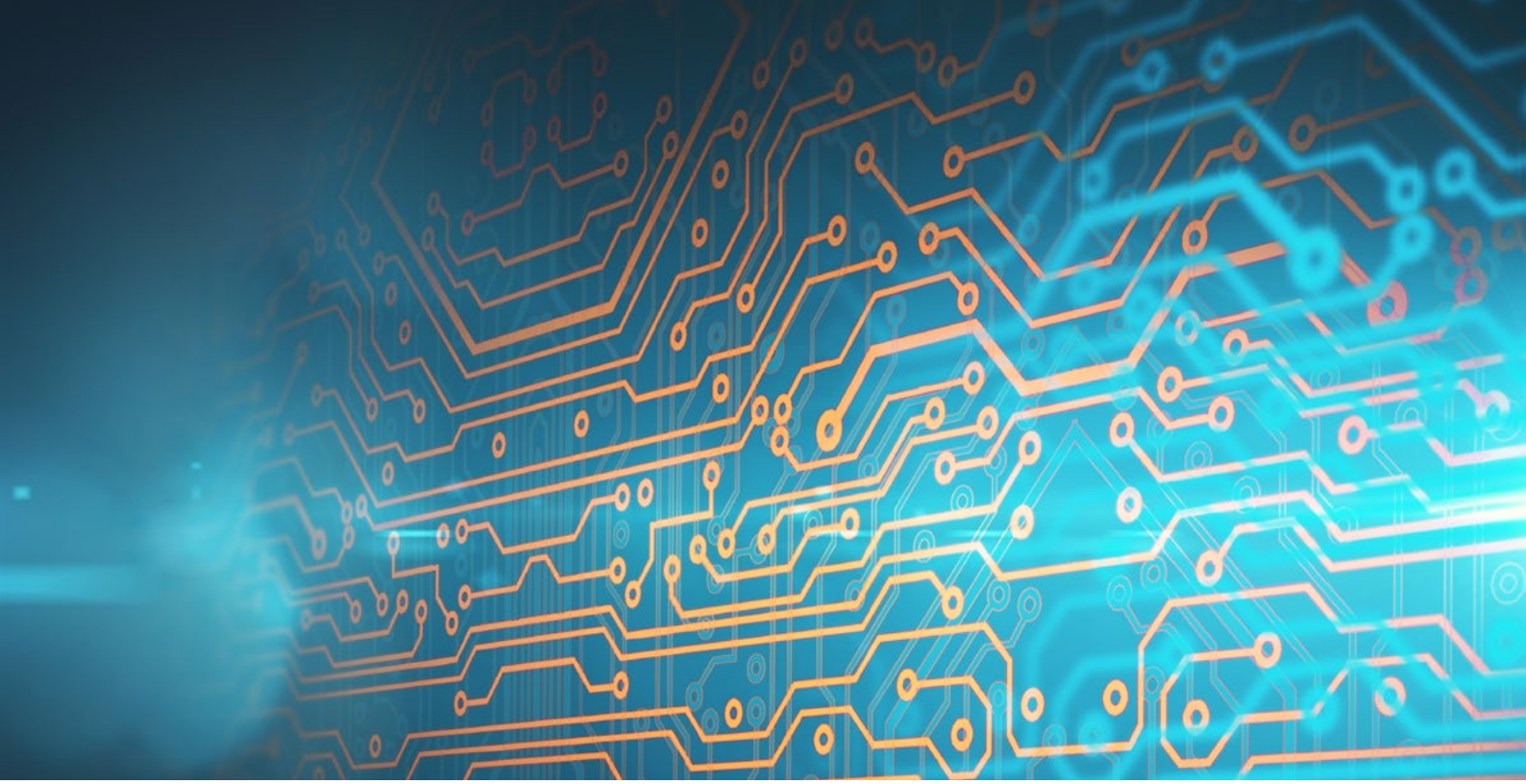
As a member of a product team developing technology for customers, you are beholden to their greatest potential and their riskiest vulnerabilities. In these guidelines, five AI characteristics are explored that developers, engineers, designers, UX professionals and programme managers should apply to their work. When designing AI, children and youth must be put *FIRST* – where AI-powered technology is built fairly, inclusively, responsibly, safely and transparently. Each of the five characteristics includes these elements – goals, the potential for harm and risk mitigation guidance – in a checklist (Figure 4), as well as further links/resources.

Applying these principles will not be easy, nor is it intended to be. Easy is not the way of great product work, so you are invited to dig in, reflect, perhaps get uncomfortable, and come out the other side with technology that respects and celebrates the most precious, cherished and vulnerable users: children and youth.

FIGURE 4 | **Checklist – Putting children and youth FIRST**

	Goals	Greatest potential for harm	Mitigate risks
Fair	Fairness for the user and their dignity are paramount	Breaches of trust and consent	Employ proactive strategies for responsible governance
	Bias in training, expression and feedback in the AI is assumed and actively addressed	Emotional and developmental harm	Use ongoing ethical thinking and imagination
	Effort is spent understanding liability	Bias, unequal access and impact	Employ ethical governance for fairness
	Threat analysis includes how the AI could be weaponized for harm		Test and train with data to understand the behaviour of the model and its areas of bias
Inclusive	Accessibility is built-in; it is not an afterthought	Exclusion by design	Build research plans, advisory councils and participant pools that represent high variability in the target audience
	"Inclusive" accounts for and celebrates neurodiversity	Bias in, bias out, bias internalized	Actively seek user experience failures that create experiences of exclusion
	Technology development cycle and testing includes feedback from children and youth		Test and train with data to understand the behaviour of the model and its areas of bias
Responsible	The technology is age-appropriate and has a cognitive-development-stage-appropriate design	Technology gone rogue	Build advisory councils and research participant pools that represent high variability in the target audience
	The technology reflects the latest learning science	Unsophisticated, inflexible AI models	Actively seek user experience failures that create negative experiences
	The technology is created with children and youth at the centre of the design and development process	Built for small, silly adults	Overcommunicate privacy and security implications
			Build conviction around the behaviour of the AI and how it might adjust to a user's development stage
Safe	The technology does no harm to customers and cannot be used to harm others	Un/intended malicious, oblique or naive usage	Conduct user research to inform scenario planning for nefarious use cases and mitigation strategies
	Cybersecurity, including the privacy and security of customer data, is a high priority	An unsafe community	Build a multivariate measurement strategy
	The potential for over-use is acknowledged and addiction mitigation is actively built in	A callous observer	Build a transparent, explainable and user data-driven relationship model between the child, guardian and technology to identify and mitigate harm
		Demographics allowed to define the user	Have the product team develop subject-matter expertise in technology concerns related to children and youth
		Data privacy and security breaches	Build a security plan that takes children's and youth's cognitive, emotional and physical safety into account
Transparent	Everyone on the team can explain how the AI works and what the AI is being used for to a novice or lay audience	Lack or obfuscation of informed consent	Confirm the terms of use are clear, easy to read and accessible to a non-technical, literate user
	Anyone who wants to understand the AI is easily able to do so	Skirted or ignored governmental rules and regulations	Clearly disclose the use of high-risk technologies, such as facial recognition and emotion recognition, and how this data is managed
		The burden of security and privacy is left to the user	Explicitly mention the geographic regions whose data protection and privacy laws are honoured by the technology
		Excluded guardians	Use more secure options as default and allow guardians to opt in to advanced features after reading their specific terms of use
			Clearly specify the age group for which the application is built
			Provide guidelines for the environment in which the technology is meant to be used
			Create alert mechanisms for guardians to intervene in case a risk is identified during usage

Source: World Economic Forum



The challenge

People active in technology – ethicists, user researchers, software developers, programme and product managers, and designers – wrote these guidelines with people like themselves in mind: developers, programme managers, technical writers, product owners, software architects, UX designers, marketing managers, and anyone else with a hand in product development. The objective is to guide you through some of the risks associated with building AI for children and youth. Admittedly, little time was spent addressing the value of AI and machine learning (ML), and the goodness that technology can bring to the lives of children and youth. The purpose of these guidelines is not to discourage the use of AI in product design; instead, it is to help bring balance to the propensity to see only the positive potential outcomes of the products built.

The challenge is to consider the other side of the AI-infused products you are building. These guidelines can be used to interrogate the work being undertaken. They will help uncover and mitigate the deficiencies and possible risks introduced in a design before customers find them. The hope is that by helping to do this, product teams can be confident in, proud of and celebrated for the responsible AI they bring into the lives of children and youth.

Definition of children and youth

There is no single definition of children and youth. They are people whose bodies and brains are still developing. Most cannot yet drive a car or hold a job. The UN defines children as people under 18 years of age. It is even possible to consider children and youth to be up to 26, since the prefrontal cortex only completes its development up to that age.[7] Children have shorter attention spans and limited vocabulary (in some cases). Age can be measured by years on this planet or abilities on tests of cognitive skills, physical dexterity or emotional intelligence. Age, like most human concepts, is not an absolute. Due to the variability of human capability relative to age, it is important to think beyond age groups and leverage instead the more reliable concepts of cognitive, emotional and physical stages[8] as a way to understand, target, communicate and market a product.

Spending much time with children and youth reveals how self-centred they can be. This is a result of brain development, and varies as a function of developmental stage.[9] This self-centredness is excellent for self-preservation but can morph into something unpleasant when children and youth encounter negative experiences. As they are quick to take credit for the sky being blue, a child might also take credit for their parents' divorce. Their self-centredness means *everything* is their fault – the good things and the bad – and their vulnerability, especially viewed through this lens, cannot be overstated. Child and youth customers will likely internalize the good and bad parts of technology. A product team's job is to work through what this means and mitigate it accordingly.

It is important to think beyond age groups and leverage instead the more reliable concepts of the cognitive, emotional and physical stages.

Social networks

Depending on your AI or product goals, you may be connecting to or building a social network inside your product. These guidelines do not deeply explore the risks of social networks for children and youth. If a product includes a social component, however, the following are recommended:

- Focus on safety: guard against nefarious actors who **will** exploit your system to gain access to children and youth for their own gains (e.g. computer viruses, child exploitation, bullying)
- Focus on fairness: design creative alternatives to embedding implicit social hierarchies into your experiences (e.g. custom avatar clothes that cost real-world money; accumulation of likes and followers)

The following information will help initiate thinking about the risks of social networks with children and youth:

- Raising Children Network (Australia), "Social media benefits and risks: children and teenagers", 22 December 2020
- Kaspersky, Kids Safety, "The dangers of social networks", 26 February 2016
- Texas A&M University, Division of Information Technology, "7 Tips for Safe Social Networking"

Overarching limitations

When it comes to researching and working with children and youth, the experience of engineers is probably limited. It is **strongly recommended** to formally consult with experts in the fields of child development, developmental science, psychology and learning sciences, among others, to evaluate AI that will be used by children and youth. Experts will be needed who can objectively ask questions about the value, safety and utility of your product, and who:

- Interrogate your AI/ML and help you understand not only the biases within it, but also ways to mitigate it
- Develop user research plans[10] that take a multivariate approach to your product questions: qualitative and quantitative methods; longitudinal research and traditional usability work; contextual inquiry and interviews; and benchmarking and scorecarding

Additionally, among the resources listed, technology design researchers whose work focuses on technology for children are cited (in particular, Jason Yip, Julie Kientz and Alexis Hiniker). Their work captures much more depth and nuance about the risks of AI affecting children than is possible to include in these guidelines.

Putting children and youth FIRST

Fair
Inclusive
Responsible
Safe
Transparent

Whenever data is collected, systems are engineered or products are sold, ethical obligations arise to be fair and honest, and to do good work and avoid harm. These obligations are all the more pressing when working with children and youth, who are among the most vulnerable members of society. Adults have a special responsibility to help them flourish and to shield them from harm. Technologies and systems powered by AI and ML could transform how people interact with each other. But they also bring potential bias, exclusion and lack of fairness to their users. With this potential for change and shift in power also comes requisite moral duties. As a result, designers, developers, maintainers, archivists[11] and researchers of AI-driven tools for children and youth are urged to be mindful of the sensitivity and ethical ramifications of their work as they design fair AI systems.

Greatest potential for harm

The news is full of examples of biased and discriminatory AI models. Without careful design, AI models can be biased and unfair, violate trust and consent, and cause emotional and developmental harm to child and youth users.

Breaches of trust and consent

While product teams should always endeavour to be worthy of their users' trust, safeguarding the health and safety of children requires them to be even more vigilant. Consent from parents/guardians and their children should be solicited before collecting data from them, and parents/guardians and children must be informed about what data is collected and how it is being used, have control over how their data circulates (as with standards such as the General Data Protection Regulation's [GDPR] "right to be forgotten"[12]) and secure access to the data once collected.

Emotional and developmental harm

Adults have a responsibility to confirm that the material shown to children is directed towards their well-being and flourishing. Children are rapidly developing their autonomy, agency, habits and relationships with technology and each other, and the way systems are designed can negatively affect this development without care and oversight.[13]

Bias, unequal access and impact

Algorithmic decision-making can all too often reinforce existing societal biases and prejudices, and cause unequal impacts across different populations. A single aggregate performance metric, such as accuracy, may fail to capture and recognize the people being punished, left out or mistreated by your system.

Risk mitigation

Employ proactive strategies for responsible governance

Just as pilots and surgeons have a preflight checklist, a simple set of factors to dwell on before starting a project can produce significant benefits and help reduce risk. This approach is favoured by Loukides, Mason and Patil in *Ethics and Data Science*,[14] and their checklist can be instantiated in software repositories via templating libraries such as deon.[15]

Some question-based checklists, such as the Berkley-Haas ethics questions (drawn from the work of Simon Longstaff[16]), draw on many existing ethical frameworks:

- Would I be happy for this decision to be on the public record?
- What would happen if everybody did this?
- How would I like it if someone did this to me?
- Will the proposed course of action bring about a good result?
- What will the proposed course of action do to my character or the character of my organization?
- Is the proposed course of action consistent with my espoused values and principles?

> Ethical governance is the practice of understanding, evaluating, questioning and updating technology based on the stated ethical goals of the product.

Last, connected with ethical checklists are vision documents, manifestos or sets of principles that lay out virtues to strive for when building AI-related systems. Helpful examples include:

- Lupi, Giorgia, "Data Humanism, The Revolution will be Visualized"
- D'Ignazio, Catherine, and Lauren Klein, *Data Feminism*, MIT Press, 2020
- Data Capitalism, "Data for Black Lives"

These checklists are just the *start* of incorporating ethics into your design; they are not complete descriptions of a project's ethical implications or sufficient proof that a project was designed ethically. Checklists are conversation *starters* rather than conversation *enders*. Designers should also be cognizant of the specific contexts of their work: checklists for one type of design may not extend to others (e.g. a preflight checklist for a pilot and a pre-op checklist for a surgeon look very different). It is your obligation as the creator of a product to research and leverage the relevant work done by others to confirm the ethical treatment of your customers.[17]

Use ongoing ethical thinking and imagination

You should build ongoing ethical evaluation into your development cycle,[18] making sure to include stakeholders from outside your team. Ideally, external stakeholders should be included who will be affected by your technology. Some strategies for carrying out these ongoing reflections can be found in Data for Children Collaborative's Ethical Assessment Tool.[19]

Employ ethical governance for fairness

Ethical product design[20] is not a one-and-done procedure: just as managers might regularly check in with their employees to see how their work is progressing, or to assess the overall health of a project, you need to regularly consider the ethical "health" of your project. Ethical governance is the practice of understanding, evaluating, questioning and updating your technology based on the stated ethical goals of the product.[21] Periodic internal assessment is crucial as the scope and execution of the work changes over time. And as people are often limited by their own individual perspectives on how work is going, your review should require periodic *external* assessment. Governance councils, ethics review boards and public feedback can identify concerns that you would have missed and provide external metrics and criteria to avoid bad outcomes during product development.

All AI is biased, and with bias comes ethical concerns. You *will* identify potential harm in this kind of exercise, and this is *not* an indication of failure! Instead, it is a problem to understand and manage. The potential harms should be explored and documented early and revisited throughout the design process and during the product's life cycle. As with other ethical considerations, stakeholders from various disciplines – and particularly experts in child development in this case – should participate in these processes. At each stage, your governance practice should include a mitigation plan for potential harms.

The potential for harm does not end when the product development cycle ends. Besides confirming that you adhere to all applicable laws and regulations related to your product, ethical governance requires that you have considered potential harms that may result from discontinued product support or availability.

Test and train with data to understand the behaviour of the model and its areas of bias

Questions to consider are:

- How has the product defined and measured the biases in the AI?
- How have these biases been remediated?
- What gaps or benefits were uncovered from the synthesis of research you conducted on your AI?

Fair
Inclusive
Responsible
Safe
Transparent

Inclusion is an essential ingredient in people's sense of emotional, psychological and physical safety. Humans are social animals who struggle to make progress on most developmental scales without a sense of community. All people crave a sense of belonging and are naturally attuned to feelings of exclusion, inclusion and the resulting uncertainty.[22] Children and youth often lack the coping skills necessary to manage negative feelings of exclusion (real or perceived). By not focusing on building an inclusive experience, you may cause cognitive, emotional or social distress and harm.[23] Feelings of exclusion can harm a child's confidence, feelings of self-worth and development.

Technology teams may be inclined to equate *inclusion* with *accessibility*. The Smart Toy Awards,[24] developed in collaboration with the World Economic Forum, defines accessibility as an AI-powered toy that's accessible for children with physical, mental and learning disabilities, including neurodiversity, and children speaking languages other than English and from other cultures. This type of inclusivity is as important as the emotional inclusivity already noted.

Greatest potential for harm

> **Feelings of exclusion can harm a child's confidence, feelings of self-worth and development.**

Any AI model internalizes the bias in its programmers and data. This can cause unintentional exclusion by design and in practice, which is particularly harmful and problematic for children and youth, who are vulnerable and require even greater care.

Exclusion by design

Technology has many forms of exclusion.[25] The words used in the interface, the complexity or learning curve of features, and the lack of accessibility features are just a few ways in which products actively exclude people who would otherwise be customers. Unlike children, adults are able to reason about states of their own or others' exclusion *(this wasn't built with me in mind; accessibility is expensive; we're too early in our product cycle to localize these strings)*. This reasoning reduces the psychological, emotional and physical harm adults feel when excluded. Children and youth, however, may not always have this perspective. The exclusion they experience may be unchecked and could result in negative feelings about themselves and their abilities.

Bias in, bias out, bias internalized

All AI is biased.[26] Data collection and sampling methods result in models and training data that reflect the inevitable flaws of a human-created system. Bias in AI can cause harm when it assumes attitudes, abilities, capabilities and beliefs that are different from the user's. When technology concludes something about the user, it runs the risk of insulting, confusing, embarrassing, excluding or demeaning the person. Something as obvious as giving female-identifying users flower patterns (not bulldozers) for their avatars' clothes is a risk to a child's sense of personal identity and enforces potentially harmful societal norms and standards. Even worse, a child born with a cleft lip might be excluded from a camera filter because bias in the training data only further isolates them from the experience of their peers.[27] The result of these biases manifesting in the experience can cause user confusion, negative self-talk or self-esteem, and reinforcement of bullying experiences.

The concept of bias in AI has been well documented; several resources can help to address the limitations in your own work:

- McKenna, Michael, "Machines and Trust: How to Mitigate AI Bias", Toptal Developers
- Manyika, James, Jake Silberg and Brittany Presten, "What Do We Do About the Biases in AI?", *Harvard Business Review*, 25 October 2019
- PwC, "Understanding algorithmic bias and how to build trust in AI", 18 January 2021
- Yenireddy, Deepti, "Breaking Gender bias In Artificial Intelligence", LinkedIn, 12 April 2017

Risk mitigation

Build research plans, advisory councils and participant pools that represent high variability in the target audience

Your product roadmap should include robust feedback loops from users, parents/guardians and education professionals at each stage of the development. It is critical that this feedback is collected early (ideally before any code is written) and that the feedback continues after the product has shipped. You should plan to collect explicit (verbal, behavioural and sentiment) feedback at each development stage from your target customers (children, youth and parents/guardians), as well as feedback on stage and age appropriateness from experts at the same cadence and with the same level of rigour as your user testing. Finally, at all stages of development and research/testing, the team must be able to answer why AI is included in the product. For every risk identified, how are you able to justify the risks the AI introduces relative to the rewards?

Actively seek user experience failures that create experiences of exclusion

You need to include children and youth in each step of the development cycle, and to continually document how the product has enabled a variety of children and youth to successfully participate. You may decide to exclude a user type. These exclusions should be documented, shared and discussed internally to build consensus, and reflected in your marketing. During product testing, design free-form *and* directed-usage user research studies which target areas already identified that could exclude children and youth from using the product as intended or desired. You should purposely push the bounds of your product before your customers do it for you.

Test and train with data to understand the model's behaviour and its areas of bias

Acknowledge that your AI is biased. Seek to understand its limitations and document how these biases could harm children and youth. How are you able to mitigate the bias? Could said mitigation inevitably introduce a new bias? What gaps or benefits were uncovered from a deeper understanding of your AI? Should these be disclosed to your customers?

Fair
Inclusive
Responsible
Safe
Transparent

The goal of this theme is to confirm that product teams have internalized their responsibilities towards the children and youth who use their products. This starts with product teams considering (and mitigating) the possibility that they may *not* have the skills or expertise to adequately evaluate the risks of introducing their AI-enabled product to children and youth. Next, product ideation, design, planning, development and testing should be grounded in age and development-stage appropriateness, with methods to test for appropriateness that reflects the latest learning science. Layered on this traditional product cycle should be considerations for the emotional, psychological and physical safety of the children and youth being targeting. Responsible AI design is an act of collaboration between the product team and their customers and their guardians, as well as experts in learning science, ethics, developmental psychology and other relevant research fields.

Greatest potential for harm

> The unpredictability, speed and fluidity of human development necessitates sophisticated AI for children and youth that can reasonably flex across stages of development.

Introducing intelligence into an otherwise static system introduces human-like characteristics, which is part of what makes AI so attractive to consumers. This is also what makes it dangerous. The brains of children and youth seek signals of love, belonging and inclusion,[28] and these signals are significantly more salient than what adults experience.[29] Therefore, children and youth will not read signals in the same way as adults.[30] Because of this, product teams must understand that children and youth are not their customer and that they could be building something which may introduce harm. As a result, they should carefully analyse the risks, seek greater understanding and develop mitigation techniques.

Technology gone rogue

When it comes to some of society's most vulnerable citizens, skirting or ignoring established regulations related to their treatment is unethical. Children and youth are not deemed capable of understanding the implications of data sharing, personal identifiable information leaks or the risks associated with granting access to their data.[31] Lack of compliance with local, state, regional and country regulations can be catastrophic for technology developers.

Unsophisticated, inflexible AI models

Human physical, emotional and cognitive development are not in sync, nor are they consistent in their speed or trajectory.[32] For example, an 11-year-old can have the body of an 18-year-old, the emotional intelligence of a 7-year-old, and the cognitive abilities of a 13-year-old. When that same 11-year-old turns 12, they could have the body of a 19-year-old, the emotional intelligence of a 10-year-old and the cognitive abilities of a 10-year-old due to a concussion they sustained. The unpredictability, speed and fluidity of human development necessitates sophisticated AI for children and youth that can reasonably flex across stages of development. This is achievable with the guidance from authorities and subject-matter experts in child development, psychology, AI and ethics.

Built for small, silly adults

Children and youth are not just physically smaller versions of adults who have limited vocabulary and less intelligence than the product team. Similar to the failures of the "pink it and shrink it"[33] approach to feminizing products made with only men in mind, not treating children as a legitimate, holistic and independent target audience carries risks.[34] The brains of children and youth are different from those of adults. This means that they are both less and more capable than an adult on a myriad of cognitive, social and physical factors. Ideally, you are able to leverage their abilities to deliver a great user experience.

Risk mitigation

Build advisory councils and research participant pools that represent high variability in the target audience

Questions to consider:

- With the product's business model in mind, how were the development stage and age appropriateness confirmed?
- Why was AI included in the product? How do you justify the risks the AI introduces relative to the rewards?
- When and how often (and not "if") have the research and testing of the product included kids, parents/guardians, teachers and subject-matter experts to confirm the developmental stage and age appropriateness?
- How does the product confirm a feedback loop for the user, parents/guardians and education professionals into future iterations, features and product roadmap?

Actively seek user-experience failures that create negative experiences

Recommendations to consider:

- Include children and youth in each step of the development cycle
- Continually document how the product has ensured that all children and youth can participate
- Allow for free-form product testing as well as directed usage; focus on areas the team has already identified as risky, which could exclude children and youth from using the product as intended/desired

Overcommunicate privacy and security implications

Questions to consider:

- How does the management of data comply with governing data laws and policies related to consumers, specifically children (i.e. GDPR,[35] Children's Online Privacy Protection Act [COPPA],[36] Age Appropriate Design Code,[37] among others)?
- How are users informed and notified of any commercial activities related to the product or third parties?
- How does the product and the use of AI enable the user to interact safely with others?

Build conviction around the behaviour of your AI and how it might adjust to a user's development stage

Questions to consider:

- Can you articulate how your product addresses the variability you expect to see in your user's development stage, and how your AI may (or may not) accommodate for that variability?
- Will your AI adjust its behaviour based on implicit signals of the developmental stage (e.g. physical dexterity, logic/problem solving ability, language ability)?
- Are users able to correct the AI if incorrect conclusions are made about the users' developmental stage?

Psychosocial development is typically predicated on feelings of safety and security.[38] Children and youth whose environments are chaotic, dangerous and unpredictable struggle to meet developmental milestones, including learning milestones, emotional regulation and bonding. This makes sense – the brain of a child at risk will allocate its precious resources to keeping itself alive above acquiring the next developmental milestone. This is a steep price for children and youth to pay, however, no matter the severity of their experience.

Children can easily find themselves in harm's way. Their underdeveloped prefrontal cortex means they are less able to predict consequences and are more impulsive, lack self-control and lack the experience to know when they are being manipulated.[39] They will seek instant gratification and may not have interest in limiting things like screen time, purchases and interaction with online strangers. For these reasons, the product team must consider themselves an ally for the children's and youth's guardians, jointly taking responsibility for protecting all users of the technology from harm.

Greatest potential for harm

> The product team must consider themselves an ally for the children's and youth's guardians, jointly taking responsibility for protecting all users of the technology from harm.

Sadly, many people, organizations and technology actors go to great lengths to harm children and youth or exploit their vulnerabilities for their own personal gain. A product team's job is to consult with experts and think through how they may be unintentionally helping malicious actors harm children and youth with their technology, and then build ways to prevent or mitigate that harm.

The greatest potential for harming children and youth with technology can include:

Un/intended malicious, oblique or naive usage

Technology can unintentionally support negative behaviours and outcomes in several ways.[40] These are often unintended oversights by product teams, but they are nevertheless your responsibility. Certain categories of use particularly concern children and youth:

- **Malicious intent**: The individual has the express intent of causing harm or using the product in a way that is dangerous to themselves or others.
- **Naivety/ignorance**: This happens when a user ignores safety warnings or intentionally takes risks without recognizing consequences. This is particularly concerning among children and youth without fully developed frontal lobes or those with alternative learning styles. See the "Transparent" section for more advice on how to mitigate these issues.
- **Oblique use**: People do not always use your creations the way you intended them to. It does not make it wrong, but it can demonstrate the creator's lack of imagination to use an opportunity to mitigate risk and make a safer product.

An unsafe community

Product teams can be naive about how their technology will be used in social situations. Only in recent years has the potential threat, toxicity and risk of social technology been illustrated. Some people who are able to hide behind technology will do and say unsavoury things.[41] People with ill intent *will* exploit your technology to access those vulnerable in your communities. Social currency, such as followers and likes, *will* be used as indicators of personal self-worth (or the lack thereof). Adults struggle with the real-world consequences of this reality, both in controlling their behaviour in an online environment and in managing the emotional fallout from upsetting online encounters. These struggles will only be amplified for children and youth.

A callous observer

If your technology facilitates conversations between the child or youth and the machine, you must anticipate cases where the user divulges information related to potential harm or risky situations (e.g. self-harm or abuse committed by an adult). You don't want your product to ignore, diminish, joke, emphasize or overreact to this input. Instead, you must decide during product development what this relationship will be, who is involved (e.g. teacher, parent/guardian, therapist, emergency services) and clearly articulate to all actors the course of escalation and resolution if a harmful scenario is detected.

Another way the technology can ignore the needs of vulnerable users is by failing to address overuse or addiction mitigation.[42] If a child or youth is obsessively using your product, will you know? Do you know what harm obsessive use or overuse could introduce to your user? Eye strain, repetitive

strain injury, emotional instability, sleep disruption, vertigo and diminished capacity to distinguish between fantasy and reality are among the unintended consequences of overusing technology.

Demographics allowed to define the user

People are more than demographics, and while they know this intellectually, they can fall victim to assuming too much about others when demographic data is available. People tend to forget that behaviour is one of the most robust data sources for predicting what they will do with technology. Because of this risk, product teams should invest in a variety of data from which to triangulate their predictions. Demographic data should be supplemented and tempered by behavioural inputs and explicit indicators of preference.

Data privacy and security breaches

Your first line of defence in keeping your customers safe is the privacy and security features that you have built into your technology. The need for robust feature development around the protection of your customers' data cannot be overemphasized. This includes but is not limited to security and privacy of in-app data. Any methods by which others can access and resell data, or exploit, embarrass, bully, financially/emotionally/physically harm or otherwise hurt your customers, should be modelled, mitigated and revisited over the product's life cycle.

Risk mitigation

Conduct user research to inform scenario planning for nefarious use cases and mitigation strategies

- **Malicious intent**: Can you detect malicious use cases? Who should be informed when these are detected? What is the child's or youth's role in notification versus the guardian? Is the technology able to suspend itself when this happens? What negative consequences will occur if auto-detection of malicious use is wrong?

- **Naivety/ignorance**: Can you detect these use cases and redirect or accommodate the user with a different interaction path? Have you built conviction into your model's interpretability? What are the potential cases where physical or emotional harm of the child or youth could occur if your technology is used naively? Do these risks need to be addressed with the guardian and/or the child or youth during set-up?

- **Oblique use**: There is no substitute for user research to detect oblique use cases, which should ideally be ethnographic and real-world usage. Early in the development cycle and continuing through release, the team and external stakeholders should brainstorm *all* the potential ways your creation may be used and the resulting unintended consequences. This data should be supplemented by actual child or youth users who are given the opportunity to use your technology however they desire.

Build a multivariate measurement strategy

No single metric can measure the fairness, inclusivity, responsibility, safety and transparency of your product. Accordingly, you need multiple indicators of your product's health, both quantitative (what happened) and qualitative (why it happened). Scepticism towards traditional product metrics of adoption and usage should also be employed, as these traditional metrics (net promoter

> When building for children and youth, you are also building for parents, teachers and guardians.

score and daily active user) are based on adult users and lack considerations for children and youth. Some recommendations for how to build this measurement strategy and whom to consult include:

- Conduct user studies, ethnography, community juries,[43] and Consequence Scanning workshops,[44] such as Judgment Call,[45] with a professional user researcher.
- Schedule design workshops to identify and address risks, and encourage engineering teams to own these strategies and solutions (e.g. use Microsoft's Harms Modeling Framework[46]).
- Confirm that metrics and optimization used for interactions are not inadvertently "addictive". For example, ask these questions: What happens if this metric hits 100%? What are the intended and unintended consequences if these metrics hit 100%? If 100% is too much, what is the right amount? Who should answer that question?

Build a transparent, explainable and user data-driven relationship model between the child, guardian and technology to identify and mitigate harm

As mentioned, when building for children and youth, you are also building for parents, teachers and guardians. You should design the guardian's experience with your technology with the same level of careful consideration as you do the child's and youth's experience. Key questions to consider for verifying that all customers have been taken into account are:

- When the tool learns about a potential harm (e.g. child self-harm, hurting others, or being hurt by a guardian, adult, or other child or youth), what does the tool do?
- In the case of security or privacy breaches, such as hacking or viruses, how are guardians informed? What action is taken on behalf of the guardian, child or youth?
- In reporting risks, what risks does the tool report, to whom, and at what cadence?
- What data is logged for regulation auditing purposes? (Refer to COPPA to understand the requirements[47])
- How can parents or guardians control or not control the technology their child uses? Are controls asynchronous or available in real time?
- Is a mechanism in place to automatically shut the tool down if a risk is identified?

Have the product team develop subject-matter expertise in technology concerns related to children and youth

All members of the development team should be engaged in building some personal expertise in child and youth development. This, however, should not replace the need to engage with experts in the fields of child psychology, development, technology, and design for children and youth. Some proactive ways to increase sensitivity and the ability to identify risk include these actions:

- Review the work of design experts in the field[48]
- Understand what can go wrong even when well-intentioned design is delivered to children and youth: The cautionary tale of the "My Friend Cayla" smart toy[49]
- Develop success metrics that are "paired"[50] for balance among user, business and technology needs

Build a security plan that takes the children's and youth's cognitive, emotional and physical safety into account

What is your plan if a hacker gets access to the system and then to your customers, their data and personal information?

- How is the data encrypted? Is it encrypted in transit or at rest?
- What sort of personal data is necessary to collect? Can it be anonymized to further protect privacy?
- Confirm that any personal/sensitive data is highly protected in case of hacking, etc. Protected data categories for children are wider-ranging than for adults.[51]

Fair
Inclusive
Responsible
Safe
Transparent

Transparency in AI can take many forms. First, there are the clear disclaimers all products must deliver to customers based on local and state regulations. Product teams are encouraged to include the proposed AI labelling system, which is part of this toolkit, in each product – both on the physical packaging and accessible online through a QR code. Products with AI for children and youth should include the following six categories and explanations to create transparency among the product, the buyer (parent/guardian or other adult) and end user (children or youth):

Age: What age or developmental stage would this product be recommended for? What material could the AI potentially expose to the user and how is this material determined to be age- and developmental-stage-appropriate?

Accessibility: How is this product accessible for children and youth of different ages and with diverse disabilities and educational backgrounds? Has the AI been trained and tested with inclusion in mind?

Camera and microphone: Does this product use either and can they be turned on and off? Is the device always observing the user or other people using the product?

Networks: Does this product allow the user to socialize with other users through networked play or a social network? How does the product create a safe and healthy social experience? What community rules and regulations are in place to confirm that a child will not be put in a dangerous situation?

AI use: How does this product use AI? How does the product's use of AI benefit the user and their experience? How does this product's use of AI pose potential risks to the user?

Data use: How is the user's data being used? Who holds this information and whom is it shared with? Where is the user's data stored and how protected is it? How does this product communicate the use of user data?

Product developers should also consider how they build their AI to encourage its responsible use. Transparency around security, privacy and permissions helps reduce or prevent unintended consequences that arise from naive usage. Designing with the goal of transparency should also manifest in the experience you build, helping establish the trust and comfort you likely want your audiences to feel towards your AI.

Finally, transparency is achieved throughout the lifetime of the product. Day 1, when the customer first unboxes and uses the technology, is fertile ground to establish honest disclosure with your user. Day 100, when the technology takes a major update with enhanced functionality, should not be ignored as another opportunity for transparency.

> **Transparency around security, privacy and permissions helps reduce or prevent unintended consequences that arise from naive usage.**

Greatest potential for harm

AI models can be inherently opaque and difficult to understand, including by children and youth as well as their parents and guardians. You do not want to design a "black box" that is impossible to understand or explain. Without proper transparency, AI can ignore laws, obfuscate consent, and exclude parents and guardians from the process. AI that lacks transparency can also put an undue burden of privacy and security on the user. Remember that transparency breeds trust, which leads to greater engagement and enjoyment with, and success of, the product.

The greatest potential for harm of AI that is not transparent includes:

Lack or obfuscation of informed consent

AI technology is usually built as a feedback loop – the back-and-forth flow of information from the user to the technology and back again. Because the technology intends to learn from its user, there is a social (and legal) contract implicit in this conversation. Accordingly, developers of AI must acquire informed consent, where the user (or parent/legal guardian) has the capacity to knowingly and willingly agree to the terms of this contract and can accept or reject it with no penalty, at any time.

> Transparency breeds trust, which leads to greater engagement and enjoyment with, and success of, the product.

A common practice in technology is to include this informed consent in the end-user license agreement. For adults, this practice works as a way to gather informed consent but, for children, it can be seen as an attempt at obfuscation. Because the stakes are so high with kids and youth, it is recommended that informed consent be an explicit, even celebrated, act in your technology. It might also need to be an act of consent for the user *and* their parent/legal guardian. For this reason, it is important to think through what each customer is consenting to, who has the capability to consent and to what, and design mechanisms for each to actively provide their agreement.

Skirted or ignored governmental rules and regulations

The responsibility to comply with local rules and regulations related to your technology is on you, the product team and the company selling the product. The country, regional, state and local rules you follow in the development of your product should be clear to your consumer.

The burden of security and privacy is left to the user

Ideally, you are able to build AI that still works well even if the security and privacy settings are enabled and turned up to their maximum settings. This is even more imperative for AI-powered technology for kids, where the default settings should be at their most restrictive and conservative for the protection of your customers. Further, it should be your responsibility to disclose both the advantages and risks of adjusting the security and privacy levers. At any stage of use, your customers should be able to understand the implications (good and bad, related to their data or the experience of the technology) of their decisions.

Excluded guardians

Any technology targeted at children and youth has two primary users: the child and their guardian. The relationship your technology builds with the guardian is as important to the safe use of AI as the technology itself. You should inform, integrate and, if possible, listen to the guardians of your user; you should inform them during product consideration so they know if your technology is right for their child (see above); and you should inform them during the set-up, where they learn the parameters of use and boundary cases of risk. And finally, you should collaborate with them in keeping tabs on usage, when boundaries are crossed or risky behaviour is detected.

Risk mitigation

Confirm that the terms of use are clear, easy to read and accessible to a non-technical, literate user

Avoid using complicated technical or legal jargon when explaining the terms and conditions of use. Keep the terms of use to a reasonable length. If either of these is unavoidable, present a simplified (perhaps even fun and engaging) version to the user that explains important points in everyday language accessible to a non-tech-literate guardian.[52]

Clearly disclose the use of high-risk technologies (e.g. facial recognition an emotion recognition) and how this data is managed

- All high-risk technologies used in the application must be presented to the guardian upfront.
- Ingestion, analysis and storage of data collected by the technology must be clearly explained, along with options for opting in/out of security and privacy options.

> The exact technologies classified as high risk will vary with time, and thus need to be revisited in both product design and methods of disclosure.

- Identify and design scenarios of informed consent for Day 1 use as well as Day 100 (when the technology may take an update with expanded functionality). Confirm that the new requests for consent (e.g. the camera is now included in the AI experience) are well designed and include guardians.

- The exact technologies classified as high risk will vary with time, and thus need to be revisited in both product design and methods of disclosure.

- The user must be informed and ideally given the option to opt out of how their data is collected for purposes of high-risk technology (i.e. whether it is used only in-app, sent to a third party, stored in the cloud, etc.).

Explicitly mention the geographic regions whose data protection and privacy laws are honoured by the technology

- Specify the regions whose data protection and privacy laws have been considered during the design and development of the application.

- Be specific in mentioning legal sections/clauses rather than using vague language.

- Revisit these at regular intervals since these laws are currently being framed and updated by most nations.

Use more secure options as default and allow guardians to opt in to advanced features after reading their specific terms of use

- Set the default options to the most secure and least intrusive to add an additional layer of safety for every user.

- Present detailed information on the technology used when the guardians decide to opt in for a feature that uses AI.

- Work through the matrix of user experience based on security feature options. For instance, how will your technology (and AI) behave if the microphone is disabled but the camera is allowed? Can you explain the outcome of this matrix to customers?

Clearly specify the age group for which the application is built

Children of different age groups have different responses to stimuli due to their developing brains.[53] Thus, it is essential that guardians be given accurate information on the developmental stage and/or age group for which the technology was built. By disclosing this level of detail you help guardians decide not only if but how to introduce a particular child to the technology.

Provide guidelines for the environment in which the technology is meant to be used

Product teams must confirm the guardian is informed of the environment of intended use (e.g. in school as part of a group activity or at home under the supervision of an adult). This not only helps with purchase decisions, but also increases the probability that the technology will be used properly and with the greatest chance of customer success and satisfaction. It is also useful to include further details, such as recommended hours of usage per week and indicators of misuse.

Create alert mechanisms for guardians to intervene in case a risk is identified during usage

The product development cycle should build threat models that include methods of misuse and risky behaviour (e.g. overuse, bullying, inappropriate content). An outcome of this threat modelling should be solutions that allow for the detection of misuse and methods of intervention, for example the high number of hours used and friend requests from unrecognized contacts. Product documentation should include the potential threats and the features guardians and users can leverage to mitigate risk, such as data consumption monitoring, visibility into in-app messages and the ability to block/report suspicious users.

References

- Brenner, Grant Hilary, "What Makes Internet Trolls Tick?", *Psychology Today*, 5 August 2019, https://www.psychologytoday.com/us/blog/experimentations/201908/what-makes-internet-trolls-tick
- Brewster, Thomas, "Child Tracker App 'Leaks 6.8 Million Texts, 1.8 Million Photos' From Kids' Phones", *Forbes*, 22 February 2016, https://www.forbes.com/sites/thomasbrewster/2016/02/22/kids-texts-and-photos-leaked-by-uknow
- Castle, Stephen, "Boris Johnson Retreats in a U.K. Exam Debacle", *The New York Times*, 15 September 2020 update, https://www.nytimes.com/2020/08/17/world/europe/england-college-exam-johnson.html
- Children & Adversity Information, sponsored by Global Children's Fund, "How they are disadvantaged: What makes kids more vulnerable"
- Chordia, Ishita, Jason Yip and Alexis Hiniker, "Intentional Technology Use in Early Childhood Education", *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, issue CSCW, November 2019, Article No. 78, pp. 1-22, https://doi.org/10.1145/3359180
- Coldewey, Devin, "After breach exposing millions of parents and kids, toymaker VTech handed a $650K fine by FTC", TechCrunch, 8 January 2018, https://techcrunch.com/2018/01/08/after-breach-exposing-millions-of-parents-and-kids-toymaker-vtech-handed-a-650k-fine-by-ftc
- Common Sense, *Technology Addiction: Concern, Controversy, and Finding Balance*, 2016, https://www.commonsensemedia.org/sites/default/files/uploads/research/csm_2016_technology_addiction_research_brief_1.pdf
- Data For Children Collaborative with UNICEF, "Our Ethical Assessment is Now Live!", 23 April 2020, https://www.dataforchildrencollaborative.com/news-from-the-unicef-data-for-children-collaborative/our-ethical-assessment-is-now-live
- Di Placido, Dani, "YouTube's 'Elsagate' Illuminates the Unintended Horrors of the Digital Age", *Forbes*, 28 November 2017, https://www.forbes.com/sites/danidiplacido/2017/11/28/youtubes-elsagate-illuminates-the-unintended-horrors-of-the-digital-age/?sh=711f7d986ba7
- Doteveryone, "Consequence Scanning – an agile practice for responsible innovators", https://doteveryone.org.uk/project/consequence-scanning
- Designing for Children's Rights Guide, https://childrensdesignguide.org
- Federal Trade Commission, "Children's Online Privacy Protection Rule ('COPPA'), Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505, Children's Privacy, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
- Finiin, Abubakar, "The Frustrating Reality of Getting A-Level Grades Without Doing Exams", *VICE*, 17 August 2020, https://www.vice.com/en/article/bv83ea/a-level-results-algorithm-uk
- Hill, Kashmir and Aaron Krolik, "How Photos of Your Kids Are Powering Surveillance Technology", *The New York Times*, October 2019, https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html
- Hoffmann, Anna Lauren, "Data Ethics for Non-Ideal Times", 30 September 2020, https://static1.squarespace.com/static/5b8ab61f697a983fd6b04c38/t/5f74b0d450b24a77b4db1996/1601482964607/Hoffmann+-+Data+Ethics+for+Non-Ideal+Times+Lecture+Notes.pdf
- IDC 2017 Workshop on Equity & Inclusivity, "Outcomes", 28 June 2017, https://idc2017equityinclusivity.wordpress.com/outcomes
- International Organization for Standardization (ISO), Popular Standards, "ISO/IEC 27001: Information Security Management", https://www.iso.org/isoiec-27001-information-security.html
- ISO Online Browsing Platform, "ISO/IEC 27002:2013(en) Information technology – Security techniques – Code of practice for information security controls", https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en
- Intersoft Consulting, "Art. 17 GDPR: Right to erasure ('right to be forgotten')", https://gdpr-info.eu/art-17-gdpr
- Kientz, Julie A., "In Praise of Small Data: When You Might Consider N-of-1 Studies", *GetMobile: Mobile Computing and Communications*, vol. 22, issue 4, December 2018, pp. 5-8, https://doi.org/10.1145/3325867.3325869
- Legal and professional standards:
  - Association for Computing Machinery (ACM), Code of Ethics and Professional Conduct, adopted 22 June 2018, https://www.acm.org/code-of-ethics
  - Intersoft Consulting, General Data Protection Regulation (GDPR), https://gdpr-info.eu
  - Liu, Feifei, "Designing for Kids: Cognitive Considerations", Nielsen Norman Group, 16 December 2018, https://www.nngroup.com/articles/kids-cognition
  - United Nations Human Rights, Office of the High Commissioner, UN Convention on the Rights of the Child, https://www.ohchr.org/en/professionalinterest/pages/crc.aspx
  - U.S. Department of Health & Human Services, "Children: Information on Special Protections for Children as Research Subjects", 18 March 2016 update, https://www.hhs.gov/ohrp/regulations-and-policy/guidance/special-protections-for-children/index.html
- Maheshwari, Sapna, "On YouTube Kids, Startling Videos Slip Past Filters", *The New York Times*, 4 November 2017, https://www.nytimes.com/2017/11/04/business/media/youtube-kids-paw-patrol.html

- Microsoft Azure, “Community jury”, 1 November 2021, https://docs.microsoft.com/en-us/azure/architecture/guide/responsible-innovation/community-jury
- Microsoft Azure, “Foundations of assessing harm”, 8 November 2021, https://docs.microsoft.com/en-us/azure/architecture/guide/responsible-innovation/harms-modeling
- Microsoft Azure, “Judgment Call”, 12 November 2021, https://docs.microsoft.com/en-us/azure/architecture/guide/responsible-innovation/judgmentcall
- Montreal AI Ethics Institute, *The State of AI Ethics: January 2021*, https://montrealethics.ai/wp-content/uploads/2021/01/State-of-AI-Ethics-Report-January-2021.pdf
- Moore, Shannon Dawn Maree, Bruno De Oliveira Jayme and Joanna Black, “Disaster Capitalism, Rampant EdTech Opportunism, and the Advancement of Online Learning in the Era of COVID19”, *Critical Education*, vol. 12, no. 2, 2021, https://ices.library.ubc.ca/index.php/criticaled/article/view/186587
- Royal Society For Public Health, “Over 1 in 10 young gamers get into debt by buying loot boxes”, 23 December 2020, https://www.rsph.org.uk/about-us/news/over-1-in-10-young-gamers-get-into-debt-because-of-loot-boxes.html
- Rubegni, E., Jason Yip and P. Baxter, “Why does he know my name?”, Exploring failure in designing AI, robots and intelligent technologies for children, Interaction Design and Children 2020 Workshop on “Creating opportunities for children’s reflections on AI, Robotics and other intelligent technologies”, 2020
- Shneiderman, Ben, “Bridging the Gap Between Ethics and Practice: Guidelines for Reliable, Safe, and Trustworthy Human-centered AI Systems”, *ACM Transactions on Interactive Intelligent Systems*, vol. 10, no. 4, 2020, https://dl.acm.org/doi/10.1145/3419764
- Specia, Megan, “Parents, Students and Teachers Give Britain a Failing Grade Over Exam Results”, *The New York Times*, 14 August 2020, https://www.nytimes.com/2020/08/14/world/europe/england-a-level-results.html
- Swauger, Shea, “Remote testing monitored by AI is failing the students forced to undergo it”, *NBC News*, 7 November 2020, https://www.nbcnews.com/think/opinion/remote-testing-monitored-ai-failing-students-forced-undergo-it-ncna1246769
- Toolkits and checklists
  - AI Now Institute, “Algorithmic Accountability Policy Toolkit”, October 2018, https://ainowinstitute.org/aap-toolkit.pdf
  - Alethicist.org, “AI Frameworks, Guidelines, Toolkits”, https://www.aiethicist.org/frameworks-guidelines-toolkits
  - Appropriating Technology, “Ten Rules of Technology”, 21 June 2019, http://appropriatingtechnology.org/?q=node/296
  - Data For Children Collaborative with UNICEF, “Our Ethical Assessment is Now Live!”, 23 April 2020, https://www.dataforchildrencollaborative.com/news-from-the-unicef-data-for-children-collaborative/our-ethical-assessment-is-now-live
  - Loukides, Mike, Hilary Mason and DJ Patil, *Ethics and Data Science*, O’Reilly Media Inc., 25 July 2018, https://www.amazon.com/Ethics-Data-Science-Mike-Loukides-ebook/dp/B07GTC8ZN7
  - Reisman, Dillon, et al., *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability*, AI Now Institute, April 2018, https://ainowinstitute.org/aiareport2018.pdf
  - Vallor, Shannon, “An Ethical Toolkit for Engineering/Design Practice”, Santa Clara University, Markkula Center for Applied Ethics, 22 June 2018, https://www.scu.edu/ethics-in-technology-practice/ethical-toolkit
- Vinney, Cynthia, “What Is Attachment Theory? Definition and Stages”, ThoughtCo, 24 October 2019, https://www.thoughtco.com/attachment-theory-4771954
- Wang, Amy, “‘I’m in your baby’s room’: A hacker took over a baby monitor and broadcast threats, parents say”, *The Washington Post*, 20 December 2018, https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say
- Whittaker, Meredith, et al., *Disability, Bias, and AI*, AI Now Institute, New York University (USA), November 2019, https://ainowinstitute.org/disabilitybiasai-2019.pdf
- Yip, Jason C., et al., “Laughing is Scary, but Farting is Cute: A Conceptual Model of Children’s Perspectives of Creepy Technologies”, CHI ‘19: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Paper no. 73, 2019, pp. 1-15, https://dl.acm.org/doi/pdf/10.1145/3290605.3300303?casa_token=d-1xrAOzDP4AAAAA

3 AI labelling system

This system promotes transparency and trust in child and youth users, their parents and guardians.

The AI labelling system (Figure 5) is designed to be included in all AI products on their physical packaging and online accessible through a QR code. Like nutritional information on food packaging, the labelling system is intended to concisely tell consumers, including parents and guardians as well as children and youth, how the AI works and what options are available to the users. All companies are encouraged to adopt this tool to help create greater trust and transparency with the purchasers and child users of their products.

FIGURE 5 | **AI labelling system**

Age

What age are the technology and content designed for?

- Range of recommended ages in years, e.g. 4-6, 7-10

Accessibility

Can users with different abilities and backgrounds use it?

- Tested with children: Y N
- Accessible for hearing impaired: Y N
- Accessible for visually impaired: Y N
- What neurodiverse users is it designed to include (e.g. autism, dyslexia)?
- What physical disabilities is it designed to include (e.g. fine motor skills, mobility)?
- What languages are supported?

Sensors

Does it watch or listen to users with cameras and microphones?

- Camera: Y N
  - If Y, can you turn it off?
- Microphone: Y N
  - If Y, can you turn it off?

Networks

Can users play with and talk with other people when using it?

- Networked play and socialization: Y N
  - If Y, can the function be turned off?

AI use

How does it use AI to interact with users?

- Facial recognition: Y N
- Voice recognition: Y N
- Emotion recognition: Y N

Data use

Does it collect personal information?

- Gathers data: Y N
- Shares data with others: Y N
- Can you control whether your data is shared?: Y N
- US Children's Online Privacy Protection Act (COPPA) compliant: Y N
- EU General Data Protection Regulation (GDPR) compliant: Y N
- UK Information Commissioner's Office (ICO) Age Appropriate Design Code compliant: Y N
- Reason for data collection (e.g. to create customized curriculum)

Source: World Economic Forum

4 Guide for parents and guardians

This guide helps decision-making about buying and using AI products for children and youth.

This guide is designed to educate parents and guardians (Figure 6) to help them understand considerations when buying AI-powered toys, devices or apps, such as video games, smart toys, smart speakers, education technology products, and more. It is also designed to supplement the AI labelling system that may accompany the product or service.

AI products use sensors and inputs to collect information about whoever uses them. The information they collect includes images, videos, patterns of use and other data. AI products then use algorithms to interpret the information. They make predictions about and suggestions for their users.

Benefits and risks

AI products have benefits. For example, they can recommend content that users might like. But AI products also have risks – they might collect information that their consumers do not want them to use or keep. These risks carry even more weight when users are children who may or may not be ready to make decisions about their digital rights, or who may not fully know or understand the impact of AI on their lives.

FIGURE 6 | Guide for parents and guardians – What to consider

	Why it matters	Things you can do
 Age - What age is it designed for?	**Know which developmental stage is appropriate for your child.** Toys and devices are designed for certain ages. If users are too young, the technology and content might be difficult for them to use and could expose them to risk. If they are too old, the technology and content might not be very interesting or fun.	Visit the product website. Learn more from other sources like Common Sense Media on choosing the right products for different ages and developmental stages.
 Accessibility - Can users with different abilities and backgrounds use it?	**The technology should work for all equally despite these differences.** Users of all abilities should be able to use technology. Some have physical or mental disabilities that require accommodations and modification. Users look different and speak different languages, which could cause problems if the AI is not well designed.	Visit the product website. Read user reviews.
 Sensors - Does it watch or listen to users with cameras and microphones?	**Find out how the technology protects privacy, such as allowing users to turn off cameras or microphones and secure information with passwords and preferences regarding data collected by these devices.** AI products use input from cameras, microphones and sensors to watch, recognize and learn from users. AI products might use facial recognition to identify your child's face or voice recognition to detect their voice. These devices and products might also store or send your information to another location or be hacked by criminals.	Visit the product website. Call the company's customer service.
 Networks - Can users play with and talk with other people when using it?	**Children should never share personal information or engage with people they don't know, and should beware of people acting with malicious intent.** Some AI products enable users to play games and talk with other people online. Playing online with others can be fun, but you should be sure that your children proceed with caution at all times.	Read about online etiquette and online safety. Talk with your children and use resources like Google's Safety Center for families and Be Internet Awesome, and other resources.
 AI use - How does it use AI to interact with users?	**Know the strengths and limits of AI decisions and suggestions, and remember that AI decisions can be wrong.** AI products might make predictions based on the data collected and your child's prior activity. This might help your child make decisions, but it also might label or misread users.	Read user reviews. Learn more about AI and how facial and voice recognition work.
 Data use - Does it collect personal information? Why? How?	**Change settings and preferences to protect your child's data. Know what kind of information AI products collect, where and how long they keep it, and who has access to it.** AI products can collect data from you and your children and store it. Your family's and child's information is very important and should be protected.	Visit the product website and call the company's customer service to learn what kind of information AI products collect, where and how long they keep it, and who has access to it.

Source: World Economic Forum

Contributors

Lead authors

Carla Aerts
Director, Digital Change, Hodder Education, and Founder, Refracted!

Amy Alberts
Senior Director, User Research, Tableau Software

Jianyu Gao
World Economic Forum AI Youth Council Member – United States

Yakaira Núñez
Vice-President, Research and Insights Platform, Salesforce

Aimee Kendall Roundtree
Professor and Associate Dean of Research and Promotion, Texas State University

Debra Slapak
Lead, Edge Thought Leadership and Innovation, Dell Technologies

Project lead

Seth Bergeson
PwC Fellow, World Economic Forum LLC

World Economic Forum LLC

Kay Firth-Butterfield
Head of Artificial Intelligence and Machine Learning

Patrick Hynes
Lead, Partner Engagement

Eddan Katz
Platform Curator

Emily Ratté
Specialist, Artificial Intelligence and Machine Learning

Conor Sanchez
Specialist, Artificial Intelligence and Machine Learning

Acknowledgements

Maria Luciana Axente
Lead, Responsible AI and AI for Good, PwC UK

Kathy Baxter
Principal Architect, Ethical AI Practice, Salesforce

Alex Beard
Senior Director, Teach For All

Charles-Edouard Bouée
Co-Founder and Managing Partner, Alpha Intelligence Capital

Jasmina Byrne
Chief of Public Policy, United Nations Children's Fund (UNICEF)

Sam Coates
Vice-President and Head, Innovation, Interactive Business, LEGO Group

Ronald Dahl
Director, Institute of Human Development, University of California, Berkeley

Ilana Golbin
Director and Lead, Responsible AI, PwC

Alison Gopnik
Professor of Psychology, University of California, Berkeley

Dave Graham
Lead, Technology Advocacy, Dell Technologies

Beeban Kidron
Founder and Chair, 5Rights Foundation

Priya Lakhani
Founder and Chief Executive Officer, CENTURY Tech

Rose Luckin
Professor of Learner Centred Design, UCL Knowledge Lab, University College London

Gary Meltzer
Managing Partner, PwC

Illah Nourbakhsh
K&L Gates Professor of Ethics and Computational Technologies, Carnegie Mellon University

Sallie Olmsted
Lead, Global Communications, i.am MEDIA

Christopher Payne
Director, Digital Responsibility, Government and Public Affairs, LEGO Group

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

Anand Rao
Global Leader, Artificial Intelligence, PwC

Aza Raskin
Co-Founder, Center for Humane Technology

Karen Silverman
Founder and Chief Executive Officer, Cantellus Group

Matthew Studley
Wallscourt Associate Professor of Technology Ethics, University of the West of England

Sherry Turkle
Abby Rockefeller Mauzé Professor of the Social Studies of Science and Technology, Massachusetts Institute of Technology

Angela Vigil
Partner and Executive Director, Pro Bono Practice, Baker McKenzie

Steven Vosloo
Policy Specialist, Digital Connectivity, United Nations Children's Fund (UNICEF)

Alan Winfield
Professor of Robot Ethics, University of the West of England

The World Economic Forum also thanks the following project community members, AI Youth Council members and other individuals who contributed their time and insights:

Sandrine Amahoro Rutayisire, Danielle Benecke, Bianca Bertaccini, Kathleen Esfahany, Joy Fakude, Marine Formentini, Matissa Hollister, Grace Knickrehm, Nupur Ruchika Kohli, Oliver Leiriao, Mariam Al Muhairi, Candice Odgers, Melanie Penagos, Chloe Poynton, Guido Putignano, Arwa Al Qassim, Pia Ramachandani, Ana Rollán, Sundar Sundareswaran, Ecem Yilmazhaliloglu

Endnotes

1. Institute of Electrical and Electronics Engineers (IEEE), "IEEE Code of Ethics", June 2020, https://www.ieee.org/about/corporate/governance/p7-8.html (accessed 1 December 2021).
2. Dignum, Virginia, Melanie Penagos, Klara Pigmans and Steven Vosloo, *Policy guidance on AI for children, Version 2.0*, United Nations Children's Fund (UNICEF), November 2021, https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children (accessed 1 December 2021).
3. World Economic Forum, "Empowering AI Leadership: An Oversight Toolkit for Boards of Directors", 2019, https://spark.adobe.com/page/RsXNkZANwMLEf (accessed 1 December 2021).
4. United Nations Human Rights Office of the High Commissioner, "Convention on the Rights of the Child", Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with article 49, https://www.ohchr.org/en/professionalinterest/pages/crc.aspx (accessed 30 November 2021).
5. Kalliomeri, Reetta, et al., *Child-Centered Design*, Save the Children, 2020, https://resourcecentre.savethechildren.net/pdf/save_the_children_child-centered_design.pdf (accessed 1 December 2021).
6. The Toy Association, "New National Survey Finds Parents Don't Always Follow Important Toy Safety Guidelines", Press Release, 7 November 2018, https://www.toyassociation.org/PressRoom2/News/2018-news/new-national-survey-finds-parents-dont-always-follow-important-toy-safety-guidelines.aspx (accessed 1 December 2021).
7. Klein, Cynthia, "Maturation of the Prefrontal Cortex", bridges 2 understanding, 5 March 2013, https://bridges2understanding.com/maturation-of-the-prefrontal-cortex (accessed 1 December 2021).
8. Stanborough, Rebecca, "Ages and Stages: How to Monitor Child Development", Healthline, 9 December 2019, https://www.healthline.com/health/childrens-health/stages-of-child-development (accessed 1 December 2021).
9. Cell Press, "Self-centered kids? Blame their immature brains", *ScienceDaily*, 7 March 2012, https://www.sciencedaily.com/releases/2012/03/120307132206.htm (accessed 1 December 2021).
10. Yukti, "10 Most Important UX Research Methods", https://www.yukti.io/10-most-important-user-research-methods (accessed 9 December 2021).
11. Society of American Archivists (SAA), "SAA Core Values Statement and Code of Ethics", August 2020 revision, https://www2.archivists.org/statements/saa-core-values-statement-and-code-of-ethics (accessed 1 December 2021).
12. General Data Protection Regulation (GDPR), "Art. 17 GDPR, Right to erasure ('right to be forgotten')", https://gdpr-info.eu/art-17-gdpr (accessed 1 December 2021).
13. Hourcade, Juan Pablo, "Interaction Design and Children", *Foundations and Trends in Human–Computer Interaction*, vol. 1, no. 4, 2007, pp. 277–392, https://www.cs.uic.edu/~i523/hourcade.pdf (accessed 1 December 2021).
14. Loukides, Mike, Hilary Mason and DJ Patil, *Ethics and Data Science*, O'Reilly Media Inc., July 2018, https://www.oreilly.com/library/view/ethics-and-data/9781492043898 (accessed 2 December 2021).
15. Deon, "An ethics checklist for data scientists", https://deon.drivendata.org (accessed 2 December 2021).
16. Longstaff, Simon, "Ethical issues and decision making", St James Ethics Centre, 1997, https://web.archive.org/web/20040920072257/http:/www.ethics.org.au/things_to_read/articles_to_read/general_issues/article_0070.shtm (accessed 1 December 2021).
17. Madaio, Michael A., et al., "Co-Designing Checklists to Understand Organizational Challenges and Opportunities around Fairness in AI", in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (CHI 2020), 2020, http://www.jennwv.com/papers/checklists.pdf (accessed 1 December 2021).
18. Gogoll, Jan, et al., "Ethics in the Software Development Process: from Codes of Conduct to Ethical Deliberation", *Philosophy & Technology*, 2021, https://link.springer.com/article/10.1007/s13347-021-00451-w (accessed 1 December 2021).
19. Data for Children Collaborative with UNICEF, "Our Ethical Assessment Is Now Live!", 23 April 2020, https://www.dataforchildrencollaborative.com/news-from-the-unicef-data-for-children-collaborative/our-ethical-assessment-is-now-live (accessed 3 December 2021).
20. Mittelstadt, Brent, "Principles alone cannot guarantee ethical AI", May 2019, https://arxiv.org/ftp/arxiv/papers/1906/1906.06668.pdf (accessed 3 December 2021).
21. Winfield, Alan, and Marina Jirotka, "Ethical governance is essential to building trust in robotics and artificial intelligence systems", Philosophical Transactions of the Royal Society A, Mathematical, Physical and Engineering Services, 15 October 2018, https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0085 (accessed 3 December 2021).
22. Association for Psychological Science, "Harlow's Classic Studies Revealed the Importance of Maternal Contact," 20 June 2018, https://www.psychologicalscience.org/publications/observer/obsonline/harlows-classic-studies-revealed-the-importance-of-maternal-contact.html (accessed 3 December 2021).

23. The St. Petersburg-USA Orphanage Research Team, "The Effects of Early Social-Emotional and Relationship Experience on the Development of Young Orphanage Children", *Monographs of the Society for Research in Child Development*, vol. 73, no. 3, 2008, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2702123 (accessed 3 December 2021).
24. Smart Toy Awards, in collaboration with the World Economic Forum, "Smart Toy Awards: Shaping the Future of Childhood", 2021, https://www.smarttoyawards.org (accessed 3 December 2021).
25. Stemler, Sam, "Top 8 Most Common Accessibility Issues to Avoid and Solve," Accessibility Metrics, 16 July 2019, https://www.accessiblemetrics.com/blog/top-8-most-common-accessibility-issues-to-avoid-and-solve (accessed 3 December 2021).
26. Whittaker, Meredith, et al., *Disability, Bias, and AI*, AI Now Institute, New York University (USA), November 2019, https://ainowinstitute.org/disabilitybiasai-2019.pdf (accessed 3 December 2021).
27. Reddy, Shivani, "The Unfortunate History of Racial Bias in Photography", https://www.slrlounge.com/unfortunate-history-racial-bias-photography (accessed 3 December 2021).
28. Hess, Robert D., and Virginia C. Shipman, "Early Experience and the Socialization of Cognitive Modes in Children", *Child Development*, vol. 36, no. 4, December 1965, pp. 869-886, https://www.jstor.org/stable/1126930 (accessed 6 December 2021).
29. Kolitz, Daniel, "Do Kids Feel Stronger Emotions Than Adults?", Gizmodo, 10 September 2018, https://gizmodo.com/do-kids-feel-stronger-emotions-than-adults-1828933152 (accessed 6 December 2021).
30. Booker, Karene, "Age changes how young children read social cues", *Cornell Chronicle*, 14 November 2013, https://news.cornell.edu/stories/2013/11/age-changes-how-young-children-read-social-cues (accessed 6 December 2021).
31. Federal Trade Commission, "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business", June 2017, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance (accessed 6 December 2021).
32. kinedu, "Children's development is not linear", 19 August 2019, https://blog.kinedu.com/childrens-development-is-not-linear (accessed 6 December 2021).
33. Contrera, Jessica, "The end of 'shrink it and pink it': A history of advertisers missing the mark with women", *The Washington Post*, 8 June 2016, https://www.washingtonpost.com/lifestyle/style/the-end-of-shrink-it-or-pink-it-a-history-of-advertisers-missing-the-mark-with-women/2016/06/08/3bcb1832-28e9-11e6-ae4a-3cdd5fe74204_story.html (accessed 6 December 2021).
34. Calvert, Sandra L., "Children as Consumers: Advertising and Marketing", *The Future of Children*, vol. 18, no. 1, Spring 2008, https://www.jstor.org/stable/20053125 (accessed 6 December 2021).
35. Complete guide to GDPR compliance, 2021, https://gdpr.eu (accessed 6 December 2021).
36. Federal Trade Commission, "Children's Online Privacy Protection Rule ('COPPA')", https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (accessed 6 December 2021).
37. ICO, "Introduction to the Age appropriate design code", https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code (accessed 6 December 2021).
38. Vinney, Cynthia, "What Is Attachment Theory? Definition and Stages", ThoughtCo., 24 October 2019, https://www.thoughtco.com/attachment-theory-4771954 (accessed 6 December 2021).
39. Children & Adversity Information, sponsored by Global Children's Fund, "How they are disadvantaged: What makes kids more vulnerable".
40. Dark Patterns, https://www.darkpatterns.org (accessed 6 December 2021).
41. Brenner, Grant Hillary, "What Makes Internet Trolls Tick?", *Psychology Today*, 5 August 2019, https://www.psychologytoday.com/us/blog/experimentations/201908/what-makes-internet-trolls-tick (accessed 6 December 2021).
42. Common Sense, *Technology Addition: Concern, Controversy, and Finding Balance*, 2016, https://www.commonsensemedia.org/sites/default/files/uploads/research/csm_2016_technology_addiction_research_brief_1.pdf (accessed 6 December 2021).
43. Microsoft Azure, "Community jury", 1 November 2021, https://docs.microsoft.com/en-us/azure/architecture/guide/responsible-innovation/community-jury (accessed 6 December 2021).
44. Doteveryone, "Consequence Scanning – an agile practice for responsible innovators", https://doteveryone.org.uk/project/consequence-scanning (accessed 6 November 2021).
45. Microsoft Azure, "Judgment Call", 12 November 2021, https://docs.microsoft.com/en-us/azure/architecture/guide/responsible-innovation/judgmentcall (accessed 2 December 2021).
46. Microsoft Azure, "Foundations of assessing harm", 8 November 2021, https://docs.microsoft.com/en-us/azure/architecture/guide/responsible-innovation/harms-modeling (accessed 6 December 2021).
47. Federal Trade Commission, "Children's Online Privacy Protection Rule ('COPPA')", https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (accessed 6 December 2021).
48. Designing for Children's Rights Guide, https://childrensdesignguide.org/ (accessed 6 December 2021).
49. Museum of Failure, "My Friend Cayla – spying doll", 2014, https://collection.museumoffailure.com/my-friend-cayla (accessed 6 December 2021).

50. Phadnis, Shree, “Develop Correct Six Sigma Project Metrics”, iSixSigma, https://www.isixsigma.com/methodology/balanced-scorecard/develop-correct-six-sigma-project-metrics (accessed 6 December 2021).

51. Future of Privacy Forum, “The Federal Trade Commission Updates to the COPPA FAQs”, 21 October 2020, https://fpf.org/blog/ftc-updates-coppa-faqs (accessed 6 December 2021).

52. The Simple EULA Project, “Fair EULA: A new step to bridge the gap between corporate and consumer”, http://simpleeulas.weebly.com/fair-eulas.html (accessed 6 December 2021).

53. Cragg, Lucy, “The Development of Stimulus and Response Interference Control in Midchildhood”, *Developmental Psychology*, vol. 52, no. 2, November 2015, https://www.researchgate.net/publication/284547902_The_Development_of_Stimulus_and_Response_Interference_Control_in_Midchildhood (accessed 6 December 2021).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org