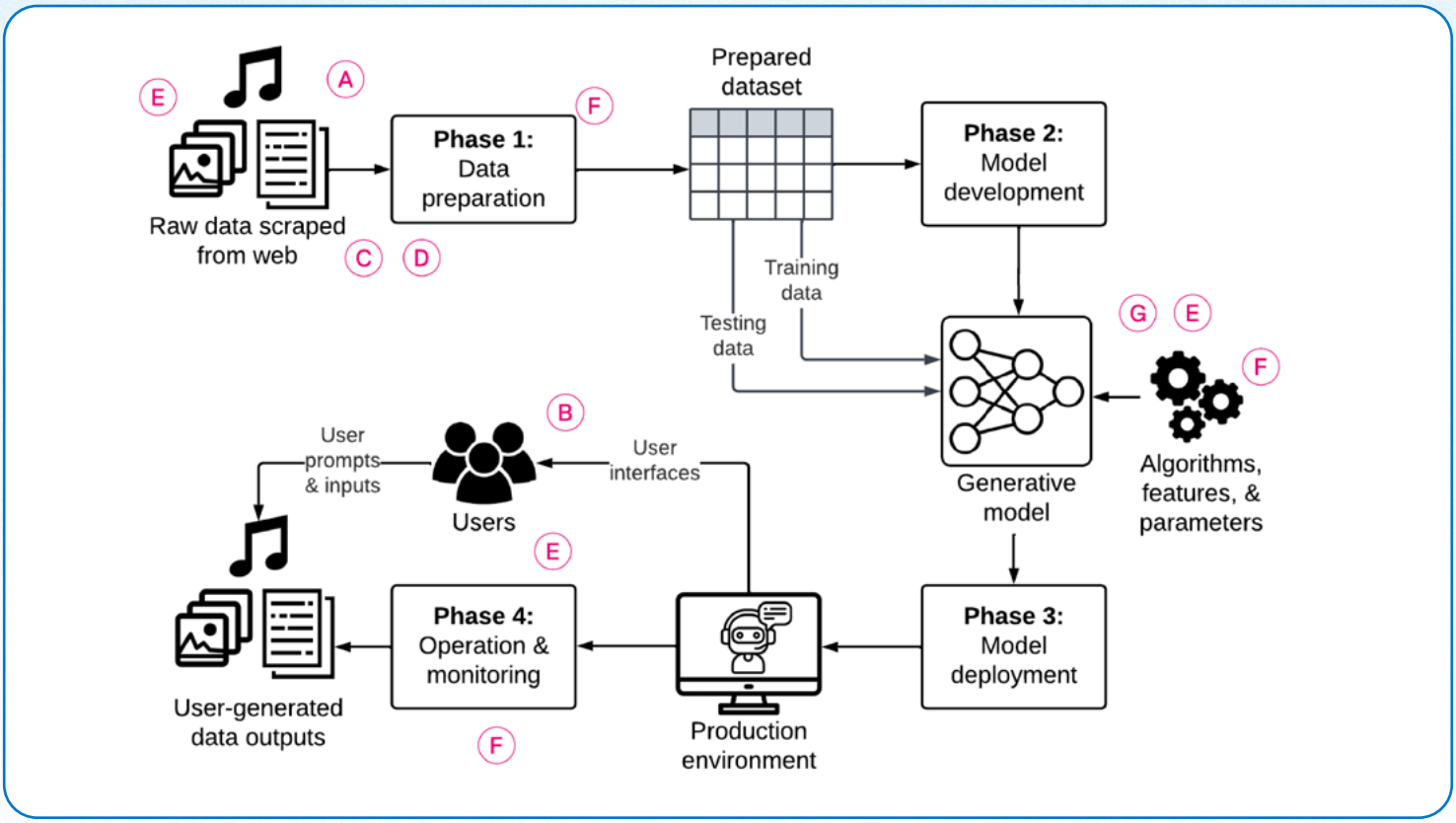
Best Practices for Safeguarding Childrens' Privacy with GenAI Tools

Read the report

This tool is designed for technologists, privacy practitioners, and policymakers looking to understand **key touchpoints** to protect children and teens' privacy in the development, maintenance, and governance of generative AI tools. It reflects the findings of a Dais study called (Gen)eration AI: Navigating Youth Privacy in the Age of GenAI.

The diagram below shows the main phases, inputs, and outputs involved in the life cycle of genAI systems, as developed by Blair Attard-Frost.[1] The diagram has been adapted to include letters, which correspond to the **best practices to address children and teens' privacy.**



The GenAI System Life Cycle

Phase 1: Data preparation consists of data collection, cleaning, labelling and curating into a large dataset for training and testing purposes.
Phase 2: Model development consists of training the model to recognize patterns in the dataset. Testing is subsequently done to ensure robustness.
Phase 3: Model deployment consists of making the model available to users on a given platform (e.g., website, app store, software, etc.)
Phase 4: Operation and monitoring consists of continuously fine-tuning the model based on users' experiences and feedback.

1 Attard-Frost, Blair, Generative AI Systems: Impacts on Artists & Creators and Related Gaps in the Artificial Intelligence and Data Act (June 5, 2023). http://dx.doi.org/10.2139/ssrn.446863.

Toronto Metropolitan University

the dais

Best Practices: Addressing Children and Teens' Privacy

The content below is inspired by Dr. Ann Cavoukian's Privacy by Design (PbD) principles,[2] and the Office of the Privacy Commissioner of Canada's principles for genAI technologies.[3] The seven PbD principles are adapted into best practices for developing and governing genAI tools for children and teens.

Developing 🔨: Technologists, Privacy Practitioners
Governing ⚖️: Policymakers, Privacy Practitioners

A. **Proactive**, not Reactive; **Preventative** not Remedial

Developing 🔨	***Governing*** ⚖️
• **Accountability mechanisms and pre-assessments are non-negotiable.** (e.g. Privacy Impact Assessments (PIAs), risk assessment frameworks, executive accountability processes, and data protection impact assessments.)	• Privacy law should set standards for clear consent mechanisms, and transparency around data collection and processing, with **specific protections** (E.g. age-appropriate wording and bite-sized language for consent) **set out for youth**. • The above standards should be paired with **accountability mechanisms** (e.g. appointing someone to be responsible for your organization's compliance) and **appropriate penalties should be established**, forming clear and strict guidelines for organizations and developers to follow.

B. Privacy as the **Default**

Developing 🔨	***Governing*** ⚖️
• **GenAI tools and features should offer the highest default privacy level for minors.** For example, chat history and model training options should be turned off by default.	• Specific youth privacy-protecting measures like simplified privacy dashboards **or a complete ban on the use of manipulative techniques such as** dark patterns in the development and interface of a tool should be set in any policy interventions governing technology, AI, and youth.

C. Privacy **Embedded** into Design

Developing 🔨	***Governing*** ⚖️
• **Decide early on what types of data your organization needs and doesn't need to collect from users.** For data that is collected, ensure mechanisms are in place to protect and honour your data processing and time limits for retention.	• **Develop regulations and policies that outline technical standards for privacy** (i.e. technical ways to operationalize privacy laws).

2 "Privacy by Design." Information and Privacy Commissioner of Ontario. (January 2018). https://www.ipc.on.ca/sites/default/files/legacy/2018/01/pbd-1.pdf.
3 "Principles for responsible, trustworthy and privacy-protective generative AI technologies." Office of the Privacy Commissioner of Canada. (December 7, 2023). https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/.

D. **Full** Functionality - Positive-Sum, not Zero-Sum

Developing 🔨	*Governing* ⚖️
• All teams - R&D, developers, privacy and cyber security, and marketing should **start with a level-setting conversation to address all interests and objectives through the lens of privacy** from the outset.	• Internal organizational policies should create **standard channels and rhythms of communication and collaboration** between privacy and security teams.

E. **End-to-End** Security - Full Lifecycle Protection

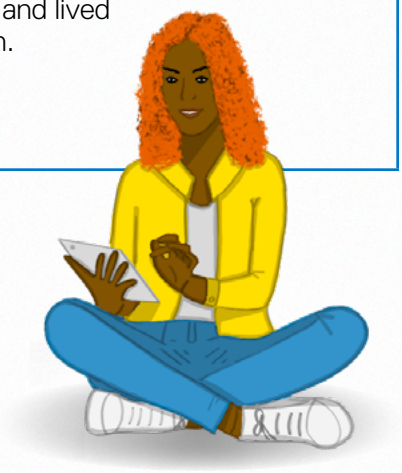
Developing 🔨	*Governing* ⚖️
• From the data that is being used to power your product, to user testing and feedback and reporting mechanisms, to ongoing maintenance and monitoring for emergent privacy threats, **youth privacy must be prioritized from ideation to use.**	• **Specific privacy policy interventions should be developed for different roles and teams.** Policy should mirror the OPC's Principles for genAI technologies which can be developed for a wide range of individuals and their responsibilities in protecting privacy.

F. **Visibility and Transparency** - Keep it Open

Developing 🔨	*Governing* ⚖️
• **Maintain clear documentation** of privacy impact assessments (PIAs), risk assessments, data protection impact assessments, and executive accountability processes for accountability purposes.	• Similar to the UK's Age Appropriate Design Code (AADC), future policy interventions should **require organizations to create age-appropriate privacy policies and terms of service** for youth.

G. **Respect for User Privacy** - Keep it User-Centric

Developing 🔨	*Governing* ⚖️
• During the R&D stage, **work alongside relevant youth-facing stakeholders**, to determine what prevalent privacy concerns and needs are, in relation to your product and its mission.	• **Develop future privacy governance and safeguards alongside educators, child development experts, and youth.** This will ensure that policy interventions are accurately reflecting the needs and lived experiences of youth.



Toronto Metropolitan University

the dais

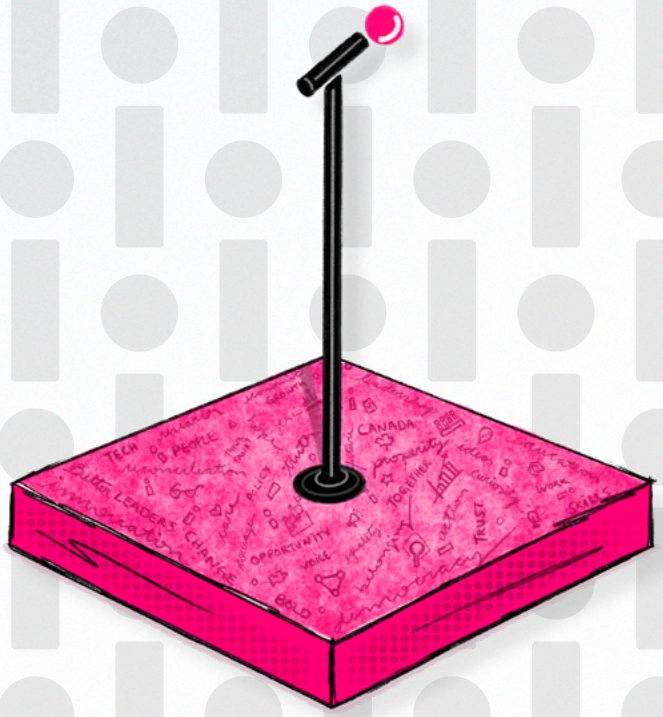
This project has been funded by the Office of the Privacy Commissioner of Canada (OPC). The views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

About the Dais

The Dais is Canada's platform for bold policies and better leaders. We are an action-oriented public policy and leadership think tank at Toronto Metropolitan University, connecting people to the ideas and power we need to build a more inclusive, innovative, prosperous Canada.

We work at the intersection of Tech + Innovation, Education + Skills and Democracy + Trust.

For more information, visit dais.ca.



Toronto Metropolitan University

the dais