

Safeguarding Tomorrow's Data Landscape with AI for Youth: A Practical Handbook



Introduction

Why this handbook?

Artificial Intelligence (AI) is rapidly transforming the way young digital citizens (ages 16–19) learn, socialize, and engage with digital technologies. While AI offers numerous benefits, such as personalized learning and entertainment, it also raises significant concerns about data privacy, informed consent, and the responsible use of personal information. This handbook aims to empower stakeholders by offering best practices and step-by-step guidance to protect youth data in AI contexts.



Who can benefit from this handbook?

- **Educators & School Administrators** – Learn how to incorporate privacy-conscious AI tools into the classroom while protecting student data.
- **Parents & Guardians** – Advocate for children's privacy rights while using AI-driven applications at home.
- **AI Developers & Researchers** – Develop responsible AI solutions that prioritize youth safety, transparency, and ethical data practices.
- **Young Digital Citizens** – Understand and exercise personal data rights when interacting with AI platforms.



Key Concepts

Personal Data

Any information related to an identified or identifiable individual (e.g., name, email, browsing history).

Informed Consent

Agreement given with an understanding of what data is collected, why, and how it will be used.



Data Minimization

Collecting only the data necessary to achieve a specific purpose, reducing unnecessary risk.

Transparency

Clear disclosures about data collection, usage, storage, and sharing practices.

Potential AI Risks for Youth

01

Data Exploitation

- **Excessive Data Collection:** AI applications may gather more data than necessary, raising the risk of misuse.
- **Third-Party Sharing:** Collected data could be shared with advertisers, analytics firms, or unknown entities.
- **Lack of Data Control:** Youth may have limited options to delete, modify, or manage their personal data, leaving them vulnerable to long-term privacy risks.

02

Profiling & Algorithmic Bias

- **Automated Decisions:** AI algorithms may create unfair profiles of young users, impacting educational opportunities or social experiences.
- **Biased Outcomes:** Historical or incomplete datasets can lead to discriminatory outcomes (e.g., lower-quality recommendations for certain groups).

03

Loss of Autonomy

- **Over-Personalization:** Constantly tailored content can shape behavior, reduce critical thinking, and limit exposure to diverse viewpoints.
- **Limited Consent Mechanisms:** Youth may lack the tools or knowledge to manage how their data is used.

Potential AI Risks for Youth

04

Data Manipulation

- **AI-Generated Deception:** AI-generated content and misinformation can manipulate opinions and spread false narratives.
- **Difficulty in Content Verification:** Young users may struggle to differentiate between authentic and AI-generated content, increasing susceptibility to online deception.

05

AI-Driven Surveillance & Tracking

- **Unregulated Facial Recognition:** AI-powered facial recognition and behavior tracking can compromise privacy, allowing unauthorized surveillance.
- **Location Data Vulnerability:** AI applications that track user locations may expose young users to security risks if data is not adequately secured or anonymized.

06

Digital Literacy & Privacy Perceptions

- **Uncertainty in AI Data Practices:** Many young users are unsure about how AI collects and uses their personal data, leading to skepticism.
- **Balancing Privacy and Convenience:** While youth value privacy, they often trade it for ease of use and personalization in digital spaces.

Best Practices

INFORMED CONSENT & AGE-APPROPRIATE NOTICES

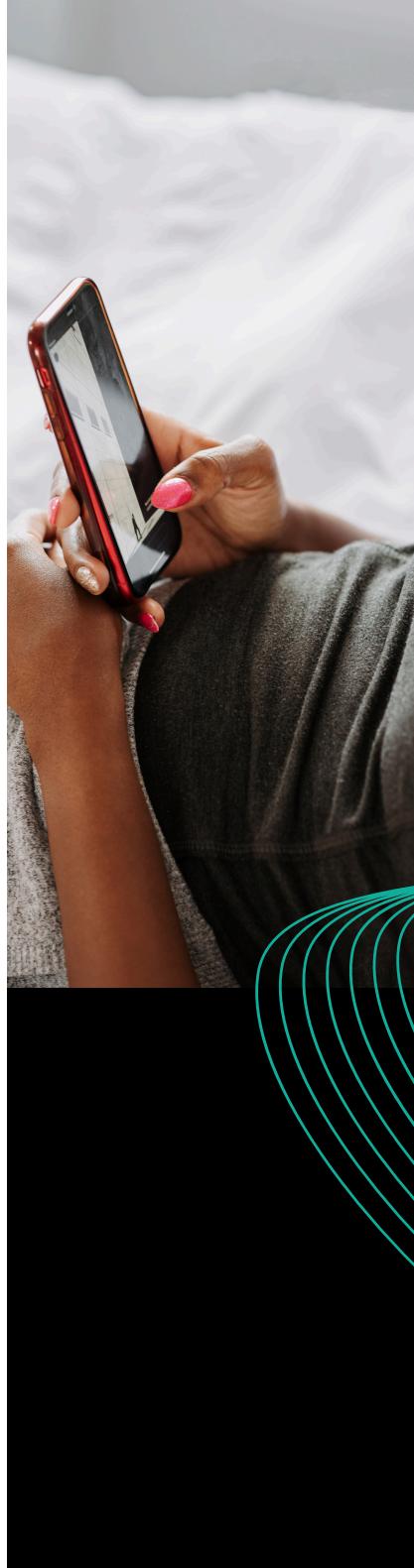
- **Clear Opt-Ins:** Provide straightforward, easy-to-understand consent forms explaining why data is collected and how it will be used.
- **Multi-Format Engagement:** Use a mix of text, visuals, and short explainer videos to improve comprehension, especially for younger audiences.
- **Ongoing Awareness:** Prompt youth to review their settings or data-sharing preferences periodically.

MULTI-STAKEHOLDER COLLABORATION FOR SAFER AI

- **Inclusive AI Policy Development:** Policymakers, educators, AI developers, and youth representatives should collaborate to design AI applications with youth privacy in mind.
- **Institutional Advocacy for AI Ethics:** Schools and institutions can champion youth-centric AI policies that prioritize fairness, security, and informed consent.

TRANSPARENCY & EXPLAINABILITY

- **Plain-Language Policies:** Use clear, jargon-free language to describe AI processes and data handling.
- **Algorithmic Transparency:** Offer general explanations of how AI makes decisions, especially for educational or recommendation systems.
- **Stakeholder Feedback Loops:** Invite regular input from students, parents, and educators regarding AI's perceived fairness and safety.



Best Practices

MONITORING & ACCOUNTABILITY

- **Internal Audits:** Regularly audit AI systems for data leaks, biases, or security vulnerabilities.
- **Reporting Mechanisms:** Encourage users to report privacy concerns or AI errors swiftly (e.g., via dedicated forms or a helpdesk).
- **Independent Oversight:** Engage neutral experts, ethicists, or advisory groups to evaluate AI's impact on youth privacy and fairness.
- **Ethical Data Handling Policies:** Establish clear policies for responsible data use, ensuring that AI systems align with privacy regulations and ethical guidelines.

PRIVACY BY DESIGN

- **Data Minimization:** Collect only essential data points needed for AI functionality.
- **Secure Storage & Transfer:** Implement encryption for data at rest and in transit, ensuring limited access.
- **User-Friendly Tools:** Offer accessible privacy dashboards where users can delete or download their data easily.
- **Anonymization:** Where possible, replace identifiable data with anonymized or aggregated or pseudonymized versions to enhance privacy while still allowing AI functionality.
- **Privacy Impact Assessments (PIAs):** Conduct privacy impact assessments to evaluate how AI systems handle data, identify risks, and implement necessary safeguards.
- **Default Privacy Protections:** Ensure that AI applications, especially those used by youth, have privacy-enhancing settings enabled by default rather than requiring users to opt in manually.



Step-by-Step Guides

EDUCATORS & SCHOOL ADMINISTRATORS

- 1. Assess AI Tools:** Review and vet AI-powered software for adherence to privacy laws and best practices.
- 2. Obtain Appropriate Consents:** If required, secure parental or guardian consent before introducing AI tools in the classroom.
- 3. Integrate Privacy Lessons:** Develop mini-lessons or modules teaching students about responsible data sharing and AI ethics.
- 4. Monitor Usage & Feedback:** Periodically check how students interact with AI software, gathering input on usability and privacy concerns.



PARENTS & GUARDIANS

- 1. Stay Informed:** Familiarize yourself with the AI apps your children use, reviewing privacy policies and data-sharing terms.
- 2. Set Boundaries:** Guide children on safe data-sharing practices, encouraging them to question the necessity of certain permissions.
- 3. Use Parental Controls:** Enable built-in parental settings or external monitoring tools where applicable, balancing oversight with respect for autonomy.
- 4. Ongoing Communication:** Discuss with your child the reasons behind privacy settings, fostering a critical awareness of potential risks.

AI DEVELOPERS & RESEARCHERS

- 1. Incorporate Privacy by Default:** Embed data minimization and secure architectures from the outset.
- 2. Conduct Impact Assessments:** Evaluate the ethical and privacy implications of AI on young users before deployment.
- 3. Engage with Youth Feedback:** Whenever possible, co-design features with the input of teenage end users to ensure real-world relevance.
- 4. Comply with Standards & Regulations:** Align development practices with OPC guidelines, PIPEDA, GDPR (if applicable), and local educational policies.

YOUNG DIGITAL CITIZENS

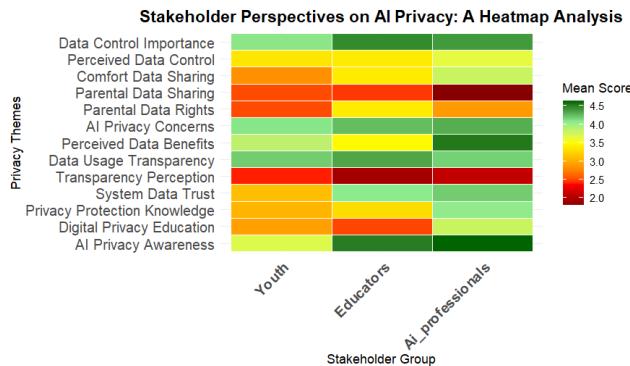
- 1. Ask Questions:** If unsure why an AI tool requests personal data, seek help from a teacher, parent, or trusted adult.
- 2. Check Settings Regularly:** Customize permissions (e.g., camera, microphone) and review your profile info to maintain control.
- 3. Identify Suspicious Requests:** Be cautious of apps asking for excessive personal details—report to a trusted adult when in doubt.
- 4. Stay Curious & Critical:** Learn basic concepts of how AI works, so you can better understand the implications of data sharing.

Evidence-Based Findings

COMPARING STAKEHOLDER PERSPECTIVES: AI PRIVACY THEMES AND MEAN SCORES

Below are key research insights derived from the project, "Safeguarding Tomorrow's Data Landscape: Young Digital Citizens' Perspectives on Privacy within AI Systems," funded by the Office of the Privacy Commissioner of Canada and led by Dr. Ajay Shrestha.

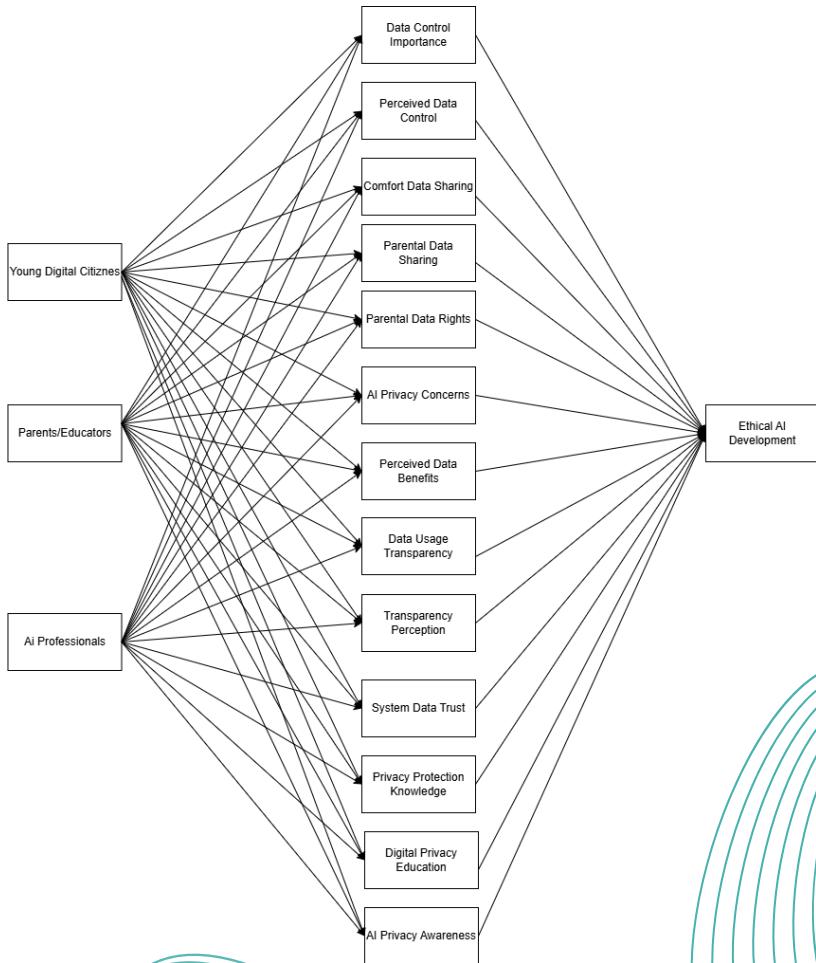
Data were collected via surveys, open-ended questionnaires, interviews, and focus groups, engaging 482 participants across three main stakeholder groups: young digital citizens, parents & educators, and AI professionals.



- Diverging Views on Data Ownership and Control:** Stakeholders differ on data control, with parents/educators and AI professionals supporting stricter governance, while youth feel less in control and hesitant to share data.
- Parental Influence vs. Youth Autonomy:** Parents/educators advocate for stronger parental rights, whereas youth and AI professionals emphasize youth autonomy in managing personal data.
- Transparency and Trust Deficit in AI Systems:** Despite valuing transparency, all groups find current AI measures lacking. Youth show the highest skepticism toward AI data governance.
- The Urgent Need for AI Literacy and Privacy Education:** AI privacy knowledge gaps persist, especially among youth and educators. Greater education and awareness are essential for responsible AI use.

Privacy Ethics Alignment in AI (PEA-AI) Model

A Stakeholder-Centric **PEA-AI** Model for AI Governance, which we developed to ensure inclusive and responsible AI oversight.



Privacy Ethics Alignment in AI (PEA-AI) Model

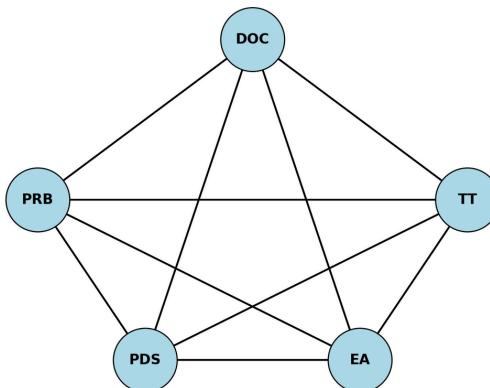
The **PEA-AI** model integrates Privacy and Ethics as core pillars, providing a structured framework for evaluating and guiding AI systems in diverse stakeholder environments.

- **Stakeholder Variations in Privacy Priorities:** Youth prioritize autonomy, parents/educators focus on security, and AI professionals emphasize compliance with ethical standards and operational efficiency. These differing priorities create tensions in AI privacy governance, as each group balances privacy concerns with their respective goals and responsibilities.
 - **Transparency and Control Gaps Across Stakeholders:** Youth worry about data tracking, educators and parents lack clear AI disclosures, and AI professionals cite technical limitations in explainability.
 - **AI Ethics as a Negotiation, Not a Fixed Framework:** Privacy governance evolves through stakeholder interactions rather than following a rigid regulatory model.
 - **The Role of Multi-Stakeholder Collaboration:** AI privacy governance requires input from youth, educators, and AI experts to align privacy measures with real-world needs.
-

PLS-SEM Findings on AI Privacy

The Partial Least Squares Structural Equation Modeling (PLS-SEM) approach was used to analyze privacy concerns among young digital citizens, parents & educators, and AI professionals. The findings, based on three SEM models, provide insights into the key relationships between:

- *Data Ownership and Control (DOC)* – Represents the extent to which individuals feel they have authority over their personal data and how it is shared or utilized within AI systems.
- *Transparency and Trust (TT)* – Examines the role of AI system transparency in fostering or diminishing trust among different stakeholders.
- *Perceived Risks and Benefits (PRB)* – Captures the dual perspectives on AI, where stakeholders assess the potential benefits against privacy-related concerns.
- *Parental Data Sharing (PDS)* – Focuses on how parents decide to share their children's data in AI systems, considering factors such as consent, awareness, and ethical concerns.
- *Education and Awareness (EA)* – Measures the level of awareness and education regarding AI privacy and its influence on perceptions of data sharing and security.



This model highlights the interconnected nature of privacy-related concerns and decisions across different stakeholder groups, demonstrating how various factors impact privacy attitudes in AI environments.

PLS-SEM Findings on AI Privacy

Model 1: Young Digital Citizens

- EA → PRB ($\beta = 0.446$, $p < 0.001$): Education plays a crucial role in shaping youth perceptions of AI risks and benefits.
- DOC → TT ($\beta = 0.306$, $p > 0.1$, NS): Youth do not necessarily associate data ownership with trust in AI.
- PRB → PDS ($\beta = 0.091$, $p > 0.1$, NS): Their risk perception does not significantly influence data-sharing behavior.
- EA → DOC ($\beta = 0.249$, $p < 0.1$): Awareness has a moderate positive effect on data ownership.
- TT → PRB ($\beta = 0.024$, $p > 0.1$, NS): Transparency does not significantly impact youth perceptions of AI risks.

Model 2: Parents & Educators

- PRB → PDS ($\beta = 0.524$, $p < 0.1$): Higher risk perception reduces willingness to share data.
- TT → PRB ($\beta = 0.331$, $p < 0.1$): Transparency enhances the balance between perceived AI risks and benefits.
- EA → DOC ($\beta = 0.429$, $p < 0.1$): Awareness strengthens data control preferences.
- EA → PDS ($\beta = 0.019$, $p > 0.1$, NS): Education does not significantly impact parental data-sharing.
- DOC → PDS ($\beta = -0.129$, $p > 0.1$, NS): Control over data does not directly influence parental data-sharing decisions.



Model 3: AI Professionals

- DOC → TT ($\beta = 0.426$, $p < 0.001$): AI experts associate strong user control with greater trust in AI.
- DOC → PDS ($\beta = -0.262$, $p < 0.01$): Those advocating for strong data control oppose broad parental data-sharing policies.
- PRB → PDS ($\beta = 0.276$, $p < 0.01$): Acknowledge the ethical considerations in data-sharing.
- EA → DOC ($\beta = 0.319$, $p < 0.01$): Education enhances data control preferences.
- TT → PDS ($\beta = -0.173$, $p < 0.1$): Transparency has a moderate negative effect on data-sharing.
- PRB → TT ($\beta = -0.173$, $p > 0.1$, NS): They do not significantly associate risk perceptions with trust.

Practical Applications

For AI Developers & Policymakers:

- Strengthen privacy-by-design principles by enhancing data control mechanisms.
- Improve AI transparency efforts to foster trust and informed decision-making.

For Educators & Parents:

- Increase AI literacy to bridge knowledge gaps and build risk awareness.
- Implement structured parental consent mechanisms that align with youth data-sharing preferences.

For Youth and End-Users:

- Advocate for AI systems with user-friendly privacy controls.
- Enhance awareness campaigns focusing on AI risks, benefits, and ethical trade-offs.

Resources

PROJECT WEBSITE



OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (OPC)

Youth Privacy Resources –
Official guides and tools.

INTERNATIONAL REGULATIONS

- **COPPA (USA):** Children's Online Privacy Protection Act sets rules for online data collection from children under 13.
- **Age Appropriate Design Code (UK):** Mandates child-focused design, high default privacy settings, and transparent data practices.
- **Digital Services Act (EU):** Increases platform accountability and transparency, with special consideration for minors' safety.
- **Model AI Governance Framework (Singapore):** Provides guidelines for responsible AI development, emphasizing transparency, fairness, user-centric design, and accountability in generative AI systems.
- **GDPR (EU):** Focuses on data minimization and consent for minors.

Conclusion

By adopting *privacy by-design* principles, **prioritizing informed consent, and fostering transparent data practices**, stakeholders can collectively create a safer digital world for young individuals. The best practices presented here are not static; they should be revisited and updated regularly in response to evolving technology, new regulations, and ongoing feedback from the youth who are directly affected by AI systems.

Next Steps:

- **Implement the recommended actions** in educational or AI development settings.
- **Collect feedback** from key stakeholders to refine and improve processes.
- **Stay informed** about emerging legislation and technical innovations that shape AI privacy standards.

By collaborating across educational institutions, families, developers, and policymakers, we can ensure that AI technologies empower young digital citizens without compromising their right to privacy and agency in the digital age.

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





CONTACT

For additional information,
guidance, or collaborations,
please reach out to:
Dr. Ajay Shrestha,
Principal Investigator
Vancouver Island University
ajay.shrestha@viu.ca