Pre-read summary

Privacy-by-Design Toolkit v0.1 — Pre-Read for Stakeholder Roundtable

Purpose of this roundtable
You are receiving this short pre-read to support a focused 90-minute discussion that will validate and refine **Privacy-by-Design Toolkit v0.1**. The Toolkit translates youth-centred evidence into practical guidance for **educators**, **parents/guardians**, **policymakers/regulators/public-sector practitioners**, and **AI professionals** (developers, product/UX, privacy engineering, governance).

What the Toolkit covers (scope)
Toolkit v0.1 focuses on **smart voice assistants and voice-enabled smart devices** (e.g., companion apps, account/device settings, voice activity controls). It prioritizes privacy-by-design recommendations that are **implementable** and **verifiable**.

What the Toolkit does not do (v0.1 boundaries)

- It does not provide legal advice or a comprehensive legal interpretation.
- It does not report new empirical results; it organizes priorities and recommendations drawn from the Toolkit's evidence base.
- It does not require participants to review any prior publications or project reports.

How priorities were organized (Tiering)

Toolkit v0.1 groups privacy concerns into Tier 1–Tier 4 using transparent criteria:

- **Severity (S):** How serious the potential privacy/autonomy harm could be for youth.
- **Frequency (F):** How consistently the concern appears across Toolkit v0.1 evidence sources (triangulated across survey themes, qualitative themes, and audit observations).
- **Feasibility (Fe):** How practical it is to address within design/governance/education actions.
- **Downstream harm potential (H):** Likelihood of secondary harms (e.g., profiling, exposure in sensitive contexts, loss of trust).

Tier intent:

- **Tier 1:** act first (highest priority; high harm + broad salience + feasible mitigation).
- **Tier 2:** act next (high priority; strong practical value; supports Tier 1).

Tier 1 priorities (confirm and refine in the roundtable)

T1-1: Clear listening/recording status + rapid stop controls
Youth should be able to tell when a device is listening/recording and stop it immediately, without hunting through settings.

T1-2: Retention/deletion and voice-history lifecycle control (time-bounded and provable)
Youth should be able to see what was stored, delete it easily, and trust that deletion occurred (including meaningful retention controls, such as auto-delete).

T1-3: Discoverable, youth-legible privacy controls (task-based "Privacy Hub")
Controls must be easy to find, easy to understand, and organized around real tasks (stop recording, delete history, manage sharing, export data, review connected devices, etc.).

Tier 2 priorities (confirm practicality and role-specific actions)

T2-1: Plain-language transparency summaries ("data labels")
Short, searchable explanations of what data is collected, why, where it goes, and how long it is kept—without policy overload.

T2-2: Bound third-party sharing and cross-service personalization
If voice data can influence ads or other services, it should be clearly disclosed and easy to control (opt-in/opt-out with verification).

T2-3: Privacy-protective defaults and meaningful consent
Non-essential data uses should not rely on hidden, preselected, or bundled choices; disabling should not be harder than enabling.

T2-4: Granular access and control (view/export/delete)
Youth should be able to access and manage voice history and related controls at the appropriate level of detail (e.g., per-item and account-wide where applicable).

T2-5: Safeguards that are strong and clearly explained
Security/privacy protections may exist but should be communicated in youth-legible language with actionable steps (e.g., account access review, connected device review).

T2-6: Practical privacy routines to build self-efficacy
Toolkit v0.1 emphasizes repeatable routines (e.g., Locate → Limit → Review → Delete → Verify) that support real protective behavior, especially where settings are complex.

What feedback is needed from you (focus of the discussion)

Please come prepared to comment on the following, from your stakeholder perspective:

- **Tier confirmation:** Validate that Tier 1 priorities reflect the most urgent concerns to address first, and note any missing items that remain within the Toolkit scope.
- **Listening/recording clarity (Tier 1):** Define the minimum acceptable "at-a-glance" listening/recording indicator and rapid stop control, and what would make it trustworthy.
- **Retention/deletion lifecycle (Tier 1):** Describe what "good" looks like for retention limits, auto-delete, and deletion confirmation.
- **Discoverability/Privacy Hub (Tier 1):** Identify the privacy tasks that must be front-and-centre, and suggest navigation or wording changes that improve youth readability.
- **Transparency summaries/data labels (Tier 2):** Specify what a short transparency summary must include (what/why/where/how long/how to control) to support meaningful understanding.
- **Third-party sharing/cross-service personalization (Tier 2):** Recommend practical ways to disclose and control these flows without creating policy overload.
- **Defaults and consent (Tier 2):** Identify settings that should be privacy-protective by default and describe what meaningful consent should look like in setup flows.
- **Verification + skills (Tier 2):** Define acceptable evidence for verifying implementation (e.g., observable UI/control, checklist items, audit tasks) and propose simple routines that build practical self-efficacy.

No other reading is required. Your feedback will be synthesized into a **Roundtable Synthesis Memo** and used to revise Toolkit v0.1 into **Toolkit v1.0**, with a brief change log.

Transcription consent

Privacy-by-Design Toolkit v0.1 — Feedback Form (Roundtable)

Stakeholder group (check one):
☐ Parent/Guardian ☐ Educator ☐ Policymaker/Regulator/Public Sector ☐ AI Professional

Email (for honorarium processing): _____

Consent (required)
☐ *I consent to transcription-only capture of this session for note accuracy (no audio or video recording). I understand live captions will be enabled but not saved.*

Feedback form (ratings + short answers)

Ratings (1–5; tick one per item)

1. Tier 1 priorities reflect the most important issues to address first.
☐1 ☐2 ☐3 ☐4 ☐5

2. "Listening/recording status + rapid stop controls" is clear and implementable.
☐1 ☐2 ☐3 ☐4 ☐5

3. "Retention/deletion + voice history lifecycle control" is clear and implementable.
☐1 ☐2 ☐3 ☐4 ☐5

4. "Discoverable, youth-legible controls (Privacy Hub)" is realistic in practice.
☐1 ☐2 ☐3 ☐4 ☐5

5. "Plain-language transparency summaries (data labels)" would improve understanding and consent.
☐1 ☐2 ☐3 ☐4 ☐5

6. "Third-party sharing/cross-service personalization boundaries" is feasible to implement and verify.
☐1 ☐2 ☐3 ☐4 ☐5

7. "Privacy-protective defaults + meaningful consent" is feasible to implement and verify.
☐1 ☐2 ☐3 ☐4 ☐5

8. The verification approach (observable indicators/checklists) is sufficient for accountability.
☐1 ☐2 ☐3 ☐4 ☐5

Short answers (brief)

A) Which one Tier 1–2 guideline would you prioritize first, and why?

_____

_____

B) What is the biggest implementation barrier (for your context) and what would make it easier?

_____

_____

C) What concrete evidence would you accept to verify implementation (e.g., UI element, policy statement, audit task result)?

_____

_____

D) What is one change you would make to improve clarity or practical usability of the Toolkit?

_____

_____

Guide (agenda)

90-minute Microsoft Teams Roundtable (Toolkit v0.1)

Session setup (before start): Enable **transcription only** (no audio/video recording). Enable **live captions** (participants' captions are not saved).

Agenda (90 minutes)

- **0–15 min** — Welcome, consent/housekeeping, objectives
  Toolkit v0.1 snapshot: scope + Tier 1–2 priorities
- **15–80 min** — Guided discussion (8 questions; implementation-focused)
- **80–90 min** — Summarize actionable edits, confirm next steps, closing