[redacted] [redacted]

CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Hello,

I hope you are well

I am so excited to see an online privacy code for children is being developed. I have worked in maximum security facilities for a long time, and it was devastating to see the harms children faced due to people exploiting them online.

Ihave included some feedback below:

13.1 Are there any additional or specific technical measures that APP entities should adopt to safeguard children's personal information from security risks, considering their heightened vulnerability?

Yes. Given children's increased vulnerability and limited capacity to understand privacy risks, APP entities should implement the following specific technical measures:

- **End-to-end encryption by default** for all data collection, storage, and transmission involving children's personal information.
- **Granular access controls** and **role-based access** within systems to ensure only authorised personnel access children's data.
- **Automated anomaly detection** tools using AI/ML to identify and respond to unusual access patterns or attempted breaches related to children's data.
- **High-privacy default settings**, including default opt-outs for profiling, location tracking, and data sharing with third parties. If messaging includes anything asking children for personal information from a new follower, it should provide a prompt or warning message to the child using the app, this can make them pause and think about their response and realise it is detected as a harmful message.
- **Age-assurance mechanisms** that are privacy-preserving (e.g. zero-knowledge proof age verification) to limit access to certain features or content.
- **ID Verification / Guardian check** Children under a certain age should require their parents ID to be scanned before setting up a profile, so it is verified their parent is aware of the account creation.
- **Secure APIs** and encrypted backend infrastructure to prevent data leaks in mobile apps and websites used by children.

13.2 Are there any additional or specific organisational measures that APP entities should adopt to safeguard children’s personal information from security risks, considering their heightened vulnerability?

Yes. Organisational safeguards are critical. APP entities should:

- **Appoint a Child Data Protection Officer (CDPO)** or include specific responsibilities within existing privacy teams to oversee risks related to children solely.
- **Develop child-specific privacy risk assessments** as part of Privacy Impact Assessments (PIAs), identifying unique threats to children’s data.
- **Implement child-specific data governance policies**, including clear protocols for handling, storing, and deleting children’s data.
- **Regular staff training** on children’s privacy laws and best practices, especially for employees involved in product development, marketing, and data analytics. Training should also include information based on recent global cases, identifying harms which have not been detected before as severe, as a learning.
- **Vendor and third-party oversight**, including requiring contracts that prohibit secondary use of children’s data and regular audits of third-party compliance.

13.3 How can APP entities ensure their data retention policies are appropriate for children’s data, including timely deletion or de-identification when the information is no longer needed?

To make data retention policies appropriate for children:

- **Set shorter default retention periods** for children’s data than adult data (e.g., 6–12 months unless legally required to retain longer).
- **Automate deletion or de-identification processes** with regular audits to ensure compliance.
- **Build user dashboards** for children and/or guardians to view, manage, and request deletion of personal information easily. Needs to be easy to find and use by children.
- **Implement “growing up” protocols**, where children’s data is reviewed or flagged for deletion or re-consent when they reach a certain age (e.g., 13 or 18).
- **Include clear, accessible explanations** for children and guardians about how long data will be kept and how it will be safely disposed of.

13.4 Do you have any specific views on how APP 11 should be applied, or complied with, in relation to the privacy of children?

APP 11 should be interpreted with heightened obligations for children due to their inability to fully understand or consent to privacy risks. Specifically:

- **Risk-based approach**: Security measures should be proportionate to the sensitivity and volume of data, with stricter standards applied to children’s data.

- **Proactive breach management**: Entities must notify guardians and the OAIC of any breaches affecting children immediately, with tailored communications for children's understanding.
- **Zero-data tolerance for unnecessary collection**: If data is not essential for the service, especially data like precise geolocation or behavioural tracking, it should not be collected at all.
- **Continuous review and adaptation**: APP 11 compliance for children should require frequent reviews of security practices as threats evolve and as children grow into new developmental stages.

I look forward to seeing the final document.

[redacted]

[redacted]