Uber

Office of the Australian Information Commissioner
Submission on the Exposure Draft of the Children's Online Privacy Code

By Email: copc@oaic.gov.au

Uber Submission: Children's Online Privacy Code

Executive Summary

At Uber, the safety and privacy of young people are our top priorities. We commend the Government for taking steps to improve online safety for children and we strongly support creating strong privacy protections for children online. However, aspects of the draft Children's Online Privacy Code risk creating unintended consequences that could reduce the effectiveness of important safety systems, increase unnecessary collection of sensitive information of children, and create operational uncertainty for services used by millions of Australians.

Uber uses data to enable features designed to protect our user's physical safety. Features such as live trip tracking, route monitoring, emergency escalation, fraud prevention and parental trip visibility are core safety tools, particularly for Teen Accounts.

The Code should preserve organisations' ability to use data for these purposes without consent requirements that undermine the effectiveness of such safety features or rigid interpretations of "strict necessity".

The Code should also avoid creating obligations for organisations to collect more personal information from children and adults than is necessary to manage the relevant risk. In particular, the Code should support privacy-preserving approaches that use existing account structures, parent or guardian involvement, age-band signals, and proportionate risk assessments, rather than defaulting to hard identity verification or applying child-level restrictions to all users.

We are also concerned that some provisions may unintentionally encourage platforms to collect more sensitive information, including government IDs or biometric data, in order to verify age or parental responsibility. This would be inconsistent with the broader privacy-protective intent of the Code.

Uber supports a practical, risk-based approach that:

- recognises existing family-linked account models;
- supports proportionate age assurance measures;
- distinguishes safety, fraud, account, support and service communications from direct marketing;
- recognises that safety, security, fraud prevention, account integrity, support and incident response may be core service uses of personal information;
- aligns the "best interests of the child" concept with international approaches by treating it as a primary design and risk-assessment consideration; and
- focuses enhanced protections on accounts known or reasonably assessed to belong to minors.

Uber's Teen Products

Uber offers family-linked teen accounts that enable teenagers aged 13–17 to request rides and order meals through a parent or guardian-managed account. These products are designed to provide age-appropriate access to mobility and delivery services with parent or guardian involvement, safety features and account-level controls. Through a family-linked account, a parent or guardian invites their teen to the platform using their own verified adult account. This creates a specialised profile linked to the parent or guardian's Family profile and payment method.

Safety is built into every step of the experience through non-negotiable, real-world guardrails. Trips cannot begin until the driver enters a unique 4-digit PIN provided by the teen, ensuring they always get into the correct vehicle. Additionally, parents receive real-time GPS tracking and live status updates for every journey or delivery, while our automated RideCheck technology continuously monitors the trip for any unexpected stops or route deviations. This offers families total transparency and peace of mind without requiring minors to surrender sensitive identity documents. These features depend on appropriate collection and use of personal information, including location, trip status, account, safety and support information. They also provide a practical example of how family-linked models can deliver age-appropriate services without requiring routine collection of government identity documents or biometric information from teenagers. Consistent with the Australian Privacy Principles, parents / guardians and teens are informed of the use and collection of their personal information for these purposes.

Key Issues with the Draft Code

1. Safety-Critical Data Uses Must Remain Permissible

The draft Code's "strictly necessary" threshold risks unintentionally restricting proactive safety features that rely on data collection and monitoring.

For mobility and delivery platforms, the same information needed for a trip / delivery is also what enables real-time safety protections. For example, Uber uses trip and location information to help confirm the user enters the correct vehicle, allow parents/guardians to follow the ride, identify unexpected route or trip events, and enable timely safety support. More information on safety features can be found here.

The Code should make clear that "strictly necessary" is not limited to the technical act of providing access to a service. It should include personal information handling that is necessary to provide the service safely, securely and reliably, including where that handling supports child safety, account integrity, fraud prevention, incident detection, emergency response or parent/guardian visibility in a family-linked account model.

The Code should expressly clarify that the following are permitted core uses of children's personal information:

- safety and emergency response;
- fraud prevention and account integrity;
- trip monitoring and incident handling;
- parental oversight features;
- support and service integrity functions;
- compliance with legal, safety and reporting obligations.

Finally, the Code should recognise that a child's "best interests" include safe mobility, parental confidence, fraud prevention, reliable support, service quality, incident response and access to safety-enhancing services. Commercial service delivery can align with a child's best interests if the feature is safe, transparent, and proportionate. Restricting personal data use for safety, fraud prevention, or incident response could actually reduce protections for children and undermine the Code's goals.

Uber

2. Age Assurance Should Be Risk-Based and Privacy-Preserving

The draft Code risks encouraging businesses to collect more sensitive information than necessary in order to verify age or parental responsibility.

If interpreted rigidly, businesses may feel compelled to request passports, licences or biometric verification simply to establish whether a user is under 18 or whether a parent has authorised an account.

Uber supports a risk-based approach to age assurance. Uber Teen Accounts operate through a parent-led onboarding model where:

- the parent or guardian initiates and authorises the account through their adult profile;
- the teen account is linked to a trusted payment method;
- parents or guardians receive trip and delivery visibility and notifications; and
- safety features are enabled by default.

These systems provide meaningful parental oversight without requiring teenagers to upload government identification documents.

The Code should clarify that:

- hard age verification is not universally required;
- parent account authentication and attestations can satisfy “reasonable steps” obligations; and
- businesses should not be required to conduct manual document review or biometric checks where lower-intrusion measures are reasonable and proportionate having regard to the nature of the service, the relevant risk and the safeguards in place.for low-risk use cases.

The Code should also recognise that reasonable age assurance may be achieved through a combination of measures, including account-based signals, self-declaration, parent or guardian attestation, family-linked account setup, age-band information and other privacy-preserving methods. This would better align with data minimisation principles than requiring each service to collect new identity information from every user.

3. The “Best Interests of the Child” Concept Should Be Clear and Workable

Uber supports the principle that children’s best interests should be central to the design and operation of services that may be used by children. However, the draft Code risks creating uncertainty if “best interests” operates as an additional legality condition for each collection, use or disclosure of a child’s personal information.

A more workable approach would be to align the Code with international approaches by treating the best interests of the child as a primary consideration in product design, privacy impact assessment, risk assessment and governance. This would allow organisations to assess privacy and safety risks holistically, rather than requiring a transaction-by-transaction assessment of whether each individual collection, use or disclosure is in the best interests of each child.

The Code should also recognise that children’s best interests may include safety, access to support, age-appropriate independence, mobility, emergency response, fraud prevention, account security and parent or guardian involvement where appropriate. These interests may vary by context and should be assessed by reference to the relevant service, user group and safeguards.

4. Safety and Service Communications

Uber supports clear consent and child-friendly opt-out requirements for genuine marketing directed at children. However, the Code should clearly distinguish direct marketing from safety, transactional, account, support, product education and service communications. For example, communications about account setup, mandatory safety onboarding, trip or delivery status, driver or delivery person details, fraud warnings, incident reports, support interactions, safety tools, feature changes and account controls should not be treated as direct marketing merely because they relate to the user's engagement with the service or encourage safer use of available features. Any requirements relating to direct marketing to children should align with the Privacy Act and provide clear, workable obligations for transparency, consent where required, and opt-out.

4. The Code Should Not Apply Child-Level Restrictions to All Adults

Uber is concerned by suggestions that businesses may need to apply privacy by default settings to all users where age cannot be conclusively determined. Applying child-specific restrictions and a higher "strictly necessary" threshold for the collection, use and disclosure of personal information across all adult accounts would significantly affect the operation of many everyday digital services and reduce functionality for Australian adults.

It could also create an outcome that is inconsistent with data minimisation by encouraging services to collect more information (e.g., government issued identification) from all users in order to avoid applying child-level restrictions universally.

The Code should instead focus enhanced obligations on accounts that are known or reasonably assessed to belong to children, supported by proportionate, risk-based and privacy-preserving age assurance measures.

Conclusion

Uber supports the objective of strengthening online privacy protections for children and teenagers.

However, the Code should avoid outcomes that unintentionally weaken safety protections, increase unnecessary collection of sensitive information, or create disproportionate compliance burdens for family-linked products designed to protect young people.

Uber recommends that the Code:

- expressly recognise safety and fraud-prevention functions as permitted uses of children's personal information;
- clarify that "strictly necessary" includes personal information handling necessary to provide a service safely, securely and reliably;
- adopt a risk-based approach to age assurance and parental consent;
- clarify that government ID and biometric verification are not universally required;
- recognise parent-linked account models as legitimate mechanisms for parental authorisation and oversight;
- distinguish safety and service communications from direct marketing;
- treat best interests of the child as an overarching governance principle, not a separate legality test for each collection, use or disclosure, and should recognise that safety-critical and child-protective features may form part of a child's best interests; and
- avoid imposing child-level privacy restrictions on all adult users by default.

Uber welcomes continued engagement with the government and the OAIC on the development of the Code.