

**Submission to The Office of the
Australian Information Commissioner**
Exposure Draft of the Children's Online
Privacy Code

5 June 2026

Submission to the Office of the Australian Information Commissioner (OAIC)

Feedback on the Exposure Draft of the Children's Online Privacy Code

ARACY contact

For any queries regarding this submission, please contact:

Adam Valvasori
Lead, Advocacy, ARACY
E: adam.valvasori@aracy.org.au

Barbara Barker
Research Manager, ARACY
E: barbara.barker@aracy.org.au

EXECUTIVE SUMMARY

The Australian Research Alliance for Children and Youth (ARACY) welcomes the opportunity to provide a submission on the Draft Children's Online Privacy Code (the Code). This submission draws directly on the perspectives of young people who participated in a recent ARACY-facilitated online workshop.

Young people expressed strong support for the intent of the Code and its focus on improving transparency, safety and control. However, participants emphasised that current online environments frequently fail to deliver meaningful privacy protections.

Across the workshop, young people consistently identified:

- **Lack of genuine consent**, due to complex, lengthy and inaccessible terms and conditions
- **Manipulative design practices** ("dark patterns"), which pressure users into accepting data collection
- **Excessive data collection and retention**, often without clear justification
- **Default settings that prioritise platform interests over safety**, particularly for location tracking and profiling
- **Limited practical control over personal data**, including deletion and withdrawal of consent.

Young people's feedback underscores a clear expectation: privacy protections should be proactive, embedded by design, and not dependent on a young person's capacity to navigate complex systems.

This submission recommends strengthening the Code to ensure:

- Privacy-by-default settings for children and young people
- Clear, accessible and age-appropriate explanations of data practices
- Stronger limits on profiling, targeted advertising and data retention
- Genuine, informed and ongoing consent mechanisms
- Practical, enforceable rights to access, control and delete personal information.

INTRODUCTION

This submission is provided by ARACY to support the OAIC in finalising a Children’s Online Privacy Code that reflects the lived experience, rights and needs of children and young people.

It aims to:

- Amplify the voices of young people in regulatory decision-making
- Provide evidence-informed insights into how the Draft Code may operate in practice
- Identify opportunities to strengthen the Code to better uphold children’s privacy, safety and wellbeing.

The submission is grounded in a children’s rights-based approach, recognising that young people are active rights holders whose perspectives must inform policies that directly affect them.

About ARACY

ARACY is a national non-profit organisation working to improve the wellbeing of children and young people in Australia. ARACY brings together research, policy and practice to promote systems-level change, with a strong focus on participation and equity.

ARACY’s approach is underpinned by:

- A commitment to children’s rights and wellbeing
- Evidence-informed policy development
- Meaningful participation of children and young people in decision-making.

Learn more at www.aracy.org.au

Overview of workshop and methodology

ARACY conducted an online ‘Young and Wise’ workshop on Wednesday 20 May 2026, with 9 participants aged 13-18 years, representing diverse geographic, cultural and lived experiences.

Participants were recruited through an open Expression of Interest (EOI) process promoted via ARACY’s website and partner networks. The EOI approach prioritised diversity of lived experience and inclusive participation.

The workshop:

- Used the [OAIC high school COP Code workbook](#) (the OAIC workbook) scenarios to guide discussion
- Focused on four key areas:
 - Targeted advertising, profiling, and fairness
 - Cookies, consent and “dark patterns”
 - Location tracking, deletion and parental controls
 - Overall Code rules and impact.
- Combined structured polling (Mentimeter), facilitated discussion and written reflections.

Selected verbatim quotes and written reflections are included in **Appendix A**.

Mentimeter outputs are included in **Appendix B**.

Participation data indicates a strong interest in privacy as an issue affecting daily life, with young people noting that their generation “live[s] our whole lives online” and therefore require stronger protections.

Across all activities, a consistent theme emerged: **young people want privacy protections that are understandable, fair, and built into systems; not dependent on individual vigilance.**

1. KEY ISSUES AND THEMES RAISED BY YOUNG PEOPLE

The following section is organised broadly in line with the OAIC workbook structure and key elements of the Draft Code.

1.1 Targeted Advertising, Profiling and Best Interests

Young people's experience

Participants described targeted advertising as:

- "creepy or invasive" (ranked as the greatest harm)
- Associated with pressure to spend money and impacts on wellbeing

Several participants expressed concern about pervasive tracking, including perceptions that devices may capture voice data for advertising purposes.

Views on acceptability

Young people did not uniformly oppose targeted advertising. However, there was strong consensus that it should only occur:

- With explicit user permission
- With clear, simple controls (e.g. "stop, start, pause")

No participants supported unrestricted use of targeted advertising.

Key insights

- Young people are particularly sensitive to loss of control rather than advertising itself
- Profiling raises concerns about fairness, influence and identity formation
- There is limited understanding of how profiling occurs, reinforcing the need for transparency.

Refer to charts 2 & 3 in Appendix B.

1.2 Consent, Cookies and "Dark Patterns"

Current behaviours

Most participants reported that they:

- Routinely click "accept all" on cookie pop-ups
- Do so due to:
 - Time pressure
 - complexity and length of information

- barriers to accessing content without consent

As one participant described, *"I just don't really feel like reading it all and it doesn't really explain what it is."* (Year 8 student, Victoria)

Barriers to meaningful consent

Young people identified that current consent mechanisms are:

- Overly complex and written in legal language
- Structured to make refusal difficult
- Often unavoidable if the user wants to access a service

Participants highlighted "you are forced to press Yes" (Year 10 student, NSW), due to the necessity of platforms for school and social participation.

What young people want

When asked what matters most for consent, participants prioritised:

- Plain-language explanations
- Clear "no" options
- Explanation of why data is needed

Young people proposed:

- Short summaries and visual explanations
- "Easy read" versions for accessibility
- Child-specific terms and conditions
- Word limits or standardised formats for policies

Refer to charts 4 & 5 in Appendix B.

1.3 Transparency and Understanding

Across all discussions, clarity and accessibility were the most consistent themes.

Young people expressed that:

Privacy information should be "for humans, not legal language" (*"Legal language only for legal - not HUMANS."* (workshop participant))

Explanations should be:

- concise
- prominent
- supported by visuals or examples

Participants emphasised that current systems:

- obscure important information
- discourage engagement
- undermine trust.

Refer to chart 6 in Appendix B.

1.4 Default Settings, Location Tracking and Safety

Location tracking

Young people strongly preferred:

- Location sharing to be **off by default**
- Activated only through active user choice
- Supported by clear warnings and reminders

Participants described significant safety concerns where:

- location data is shared widely
- platforms allow unknown users to access information

Default privacy settings

There was broad agreement that:

- high privacy settings should be automatic for young people
- data collection should be minimised unless actively enabled

This aligns closely with the Code's intent around "best interests" and "privacy by default".

Refer to chart 7 in Appendix B.

1.5 Data Minimisation, Retention and Deletion

Concerns

Young people raised concerns about:

- Data being retained "longer than needed"
- Sensitive data (e.g. face images) being stored unnecessarily
- Risks associated with data breaches

Expectations

Participants clearly articulated a desire for:

- Immediate or time-limited deletion of unnecessary data
- Stronger control over removal of posts, images and accounts
- Transparent processes for deletion

Young people identified **images** and **posts** as among the most important data types to be easily deleted.

1.6 Control, Autonomy and Parental Involvement

Views on parental controls varied.

Some participants emphasised the need for:

- parental involvement for younger users
- protections against exploitation and harm

Others stressed the importance of:

- autonomy
- the ability to explore identity without surveillance

Responses to age thresholds were mixed, with no clear consensus.

This suggests the need for:

- flexible, graduated approaches
- recognition that maturity varies between individuals of the same age.

Refer to chart 8 in Appendix B.

1.7 Complaints and Accountability

Young people indicated they are most likely to:

- report issues to the platform itself
- seek support from parents or peers

However:

- awareness of external complaint pathways is limited
- confidence in enforcement mechanisms appears low.

Participants ranked:

- “no tricks to get my permission”
- “easy ways to complain”

as among the most impactful Code rules.

Refer to chart 9 in Appendix B.

1.8 Overall priorities for the Code

When asked what the Code must “get right”, young people highlighted:

- No manipulation or “trickery”
- Clear, accessible explanations
- Strong default privacy settings
- Minimal data collection
- Meaningful control over personal information

Young people expect the Code to deliver:

- more control by users
- clearer explanations
- simpler settings

Refer to charts 10-12 in Appendix B.

2. IMPLICATIONS FOR THE DRAFT CODE

The feedback suggests that while the Draft Code is well-aligned with key issues, implementation detail will be critical.

In particular:

- Transparency obligations must be operationalised in accessible formats, not just high-level requirements
- Best interests obligations must translate into enforceable design choices, especially defaults
- Consent provisions must address real-world pressures, including time constraints and access barriers
- Accountability mechanisms must be visible and usable by young people.

Importantly, young people’s feedback reinforces that:

Privacy cannot depend on a child’s ability to understand complex systems, it must be built into those systems.

3. RECOMMENDATIONS

ARACY recommends that the OAIC strengthen the Draft Code to:

1. Embed privacy by default

- Require high privacy settings for children by default
- Mandate easy to understand and access opt-in (not opt-out) for data collection, profiling and advertising

2. Strengthen transparency requirements

- Require layered, age-appropriate explanations
- Mandate “easy read” summaries and visual formats
- Introduce standardised formats for privacy notices

3. Ensure genuine consent

- Require clear, equally prominent “accept” and “decline” options
- Prohibit design practices that pressure or manipulate decisions
- Require ongoing consent when practices change

4. Limit data collection and use

- Restrict profiling and targeted advertising for children
- Require strict data minimisation
- Prohibit unnecessary sharing with third parties

5. Introduce stronger data retention and deletion rules

- Require deletion of data when no longer needed
- Set clear limits on retention of sensitive data (e.g. biometrics)
- Provide simple, accessible deletion tools

6. Improve controls and settings

- Ensure privacy settings are easy to find and use
- Provide simple controls to pause, stop or withdraw consent
- Include clear notifications for location sharing

7. Enhance safety and protections

- Require location tracking to be off by default
- Mandate safeguards against unwanted contact from unknown users

8. Support children's participation and education

- Require platforms to provide accessible education on privacy
- Ensure ongoing engagement with young people in implementation and review

9. Strengthen accountability and complaints mechanisms

- Require simple, visible reporting pathways
- Ensure responses are timely and child-friendly
- Increase awareness of regulatory complaint options.

4. CONCLUSION

Young people participating in this workshop demonstrated a strong understanding of online privacy risks and a clear expectation that systems should do more to protect them.

Their feedback highlights a fundamental principle for the Code:

Children's privacy must be protected by design, not left to chance.

ARACY welcomes the OAIC's work in developing the Draft Children's Online Privacy Code and encourages the integration of these lived experience insights to ensure the Code is practical, effective and responsive to the realities of young people's digital lives.

Appendix A: Selected verbatim quotes and written reflections

1. EOIs: What matters most to you about privacy for young people?

"We live our whole lives online unlike any previous generation and so we need to protect our privacy from a young age meaning we need laws to help us." (Year 7 student, NSW)

"That young kids don't get baited falling into older people traps." (Year 8 student, NSW)

"Keep kids safe from people who use our socials and games to trick us." (Year 9 student, NSW)

"That young people will not be exploited by TOS of platforms that no one reads. (Like how snapchat has access to your location 24/7 even if it's turned off, it's hidden deep in its TOS that no one reads)." (Year 10 student, NSW)

"Understanding about privacy among young people in the group settings. Any information & pics etc shared on one platform with one person doesn't mean it can be shared among the group of friends. Not everyone in my group might be my friend. My information needs to be protected and only shared with my permission." (Year 11 student, WA)

"Accessibility and freedom of information provision." (Year 12 student, NSW)

"I am really concerned about kids' privacy on social media platforms, and the way that kids are almost forced to compare their lives with others. I believe that kids deserve the privacy to live their own lives, without having to feel bad for where they are in life or what they are doing." (Year 12 student, Qld)

"What matters most to me is that young people feel safe having control over their own information, like who sees it and how it's used. Young people are still figuring out who they are, and they need space to explore that without fear of being exposed or having their information misused. This is especially important for those from marginalised communities!" (Year 12 student, SA)

2. Workshop discussion: Defining 'online privacy'

[Also refer to Appendix B, Chart 1]

- "safety"
- "consent"
- "protection"
- "respect"

- *"the opposite of Google"*

3. Workshop discussion: Targeted Advertising, Profiling, and Best Interests

"The privacy policy [Code] should have laws for what they need to outline, and have a word limit." (Year 7 student, NSW)

[Re. Zara's face on the bus scenario]: "It's a bit on them for exposing themselves and like putting photos (of them) on the internet. But it's also... half the person's fault that actually put it on the bus because it's like taking advantage of them." (Year 8 student, NSW)

"What's more creepy with the advertising is that if you start talking about dog toys, dog toys, dog beds... your computer will hear you and the browser will use that information." (Year 10 student NSW)

"What is it hearing when I am at school talking with my student counsellor? What is it hearing when I am arguing with someone? What does it hear when you are having a conversation that is really important? It hears all that stuff and no one knows about it." (Year 10 student, NSW)

"The majority of the responsibility lies in that company to ensure that lack of consent is coming from the responsible guardian, because this is just a child under the age of 18." (Year 12 student, SA)

"Clear, plain language would go like a mile in explaining what you're actually agreeing to." (Year 12 student, SA)

"Clarity is very important." (as a core protection) (Year 12 student, SA)

4. Workshop discussion: Dark patterns, cookies, unreadable settings/ policies

"Should they do a separate set of T's and C's that's, like, more concise for kids?" (Year 7 student, NSW)

"A lot of the time, I'm in a hurry, don't have the time, and I just have to press agree." (Year 7 student, NSW)

"I often customise my cookie settings... but they often just give me a thing saying, oh, they either take me to the really long privacy... or they'll just give customise them, and I have to scroll through 30 and say if I want them or don't want them." (Year 7 student, NSW)

"It gives me a time limit and I sometimes have to click 'accept all' or something. So there's like a time limit basically and I have no time to read it all." (Year 8 student, NSW)

"I just don't really feel like reading it all and it doesn't really explain what it is."
(Year 8 student, Victoria)

"Some people might not be able to like understand the question, and so you just click any answer just because you want to get to the next part." (Year 8 student, NSW)

"I think usually kids don't really understand what cookies are and they always just press 'allow all' instead of just like 'none' or 'necessary only'... they all just press 'allow all' for the sake of getting past that page to get what they want."
(Year 10 student NSW)

"They purposely... add so much information there, so the average person can't read it." (Year 10 student NSW)

"It's very confusing because, you know, being 17, you know, I've just never thought to myself, let's have a look at what these actually are." (Year 12 student, SA)

"I've never really like had a thought about what cookies actually do... I think it would be better if it had like a brief description of what they're actually accessing through you accepting them." (Year 12 student, NSW)

"Can I just click none at all and the website function normally? Would I have access to the same information? Or does it actually change the way that I can click on links and go to different pages?" (Year 12 student, SA)

"Make an easy read version for people with disabilities, neurodivergent people, or even everyday people who just want a quick way to read." (Mentimeter quote, workshop participant, aged 13-18 years)

5. Workshop discussion: Location tracking, deletion, parental controls

"I think permanent deletion should mean like they've gotten rid of it to the best of their abilities." (Year 7 student, NSW)

"I think people should be able to control some privacy settings when they're like 12 or 13 and then like some when they're like 15, 16." (Year 7 student, NSW)

"I feel like at 13... you should be able to change your own settings, privacy settings or what you want." (Year 8 student, NSW)

"Snapchat for a long time... your location is on by default, like telling all your friends where you are exactly, and you know, Snapchat encourages you to find random strangers, so random strangers can see your location." (Year 10 student NSW)

"Permanently deleted should mean what the English dictionary means: Permanently deleted, it cannot be accessed anywhere." (Year 10 student NSW)

"If you need parental permission to click yes or no to those kinds of things, it's just so impractical. [But] There are some privacy settings... appropriate for a parent to have access to, such as location sharing." (Year 12 student, SA)

Appendix B: Mentimeter outputs from workshop with young people

Chart 1: What does online privacy mean to you?



Chart 2: Ranking: When you see personalised or targeted ads, what feels like the biggest harm?

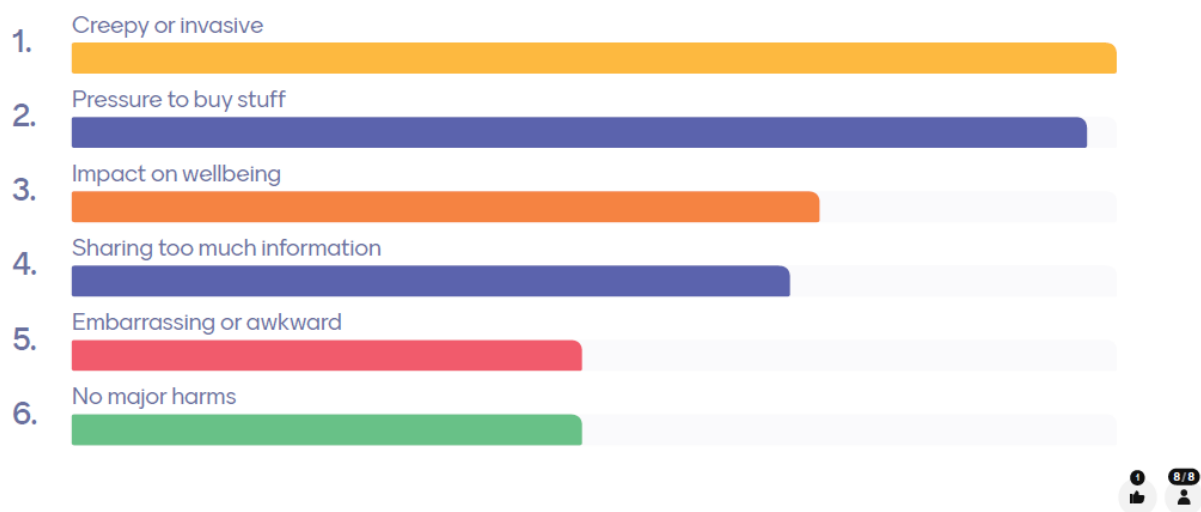


Chart 3: Targeted ads based on your interests should be allowed...



Chart 4: How could online services better explain what they do with your personal information?"



Chart 5: For me to give an online service my permission or consent, I most want them to...

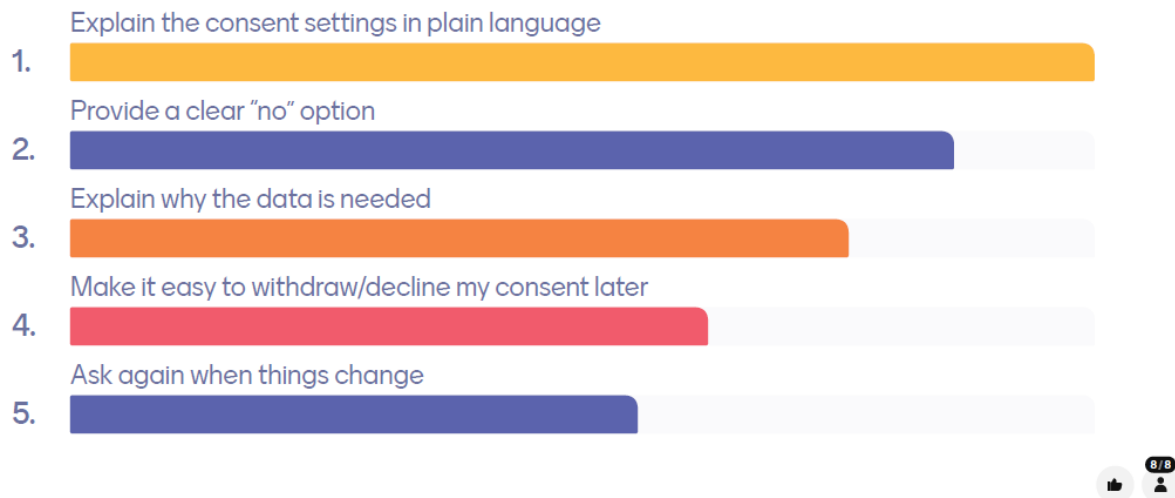


Chart 6: Location sharing for teens should be...

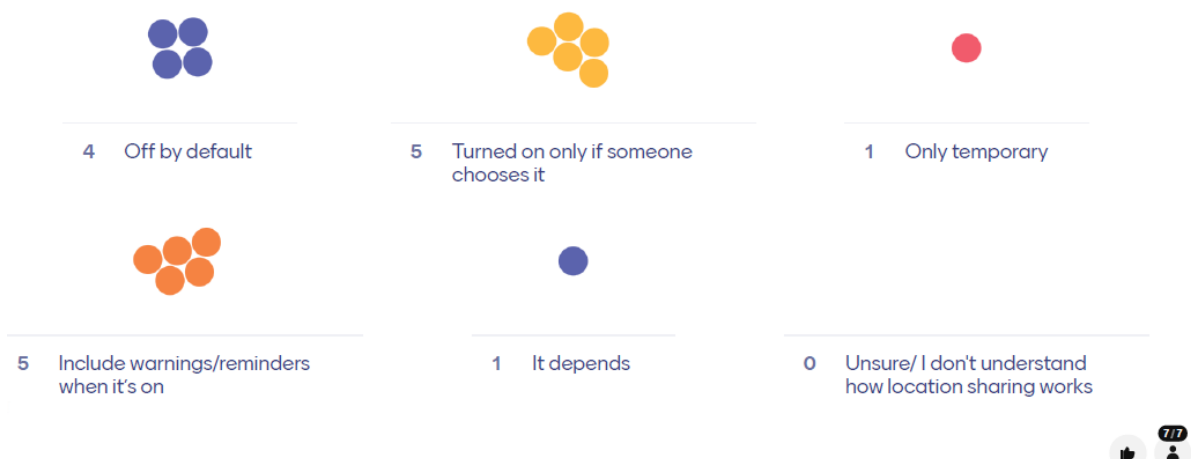


Chart 7: The easiest personal information to delete should be...



Chart 8: At what age should a young person be able to control privacy settings *without* needing parent/carer permission?

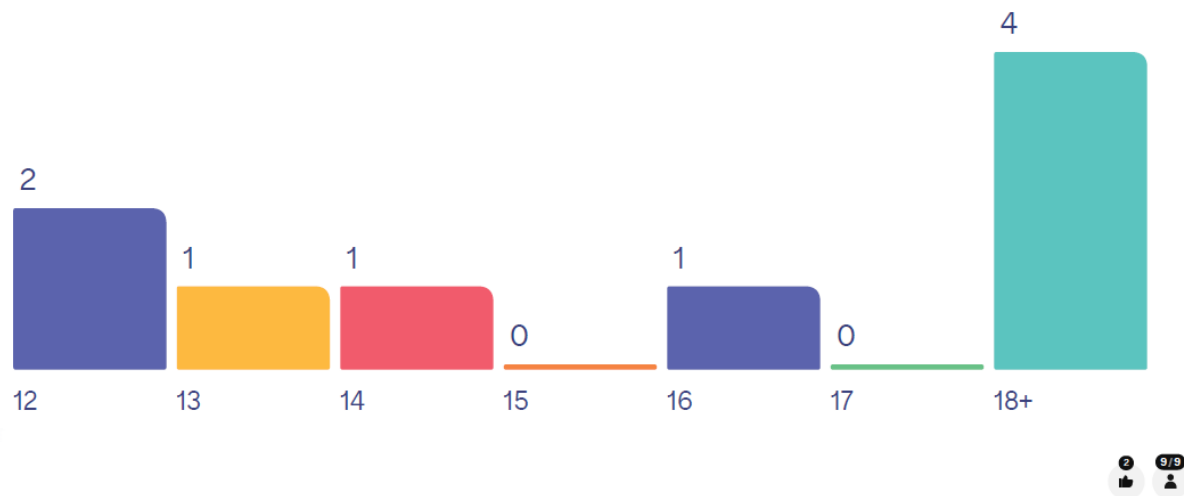


Chart 9: If you had a negative experience online, what would you do?

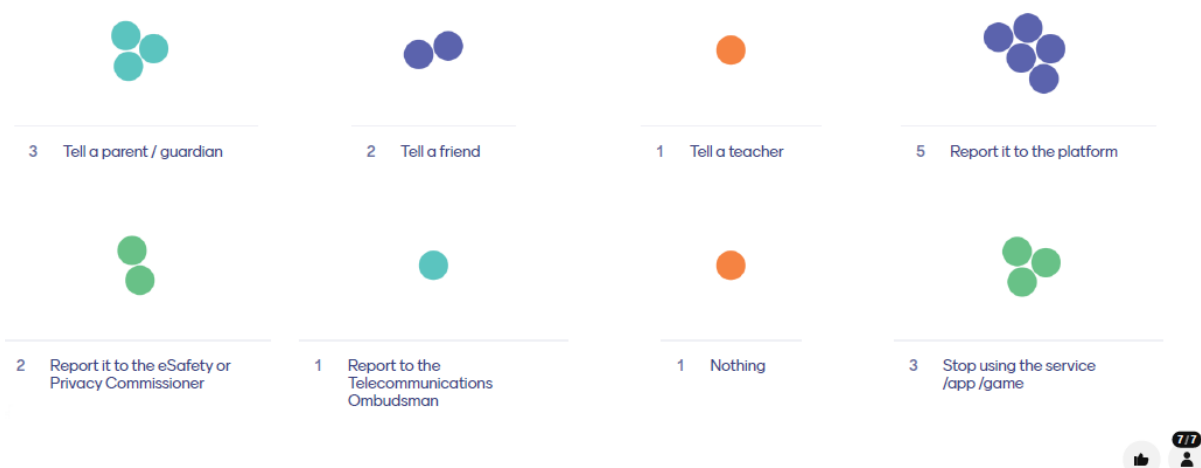


Chart 10: Rank which of the Code's rules is likely to have the greatest impact on your online privacy?

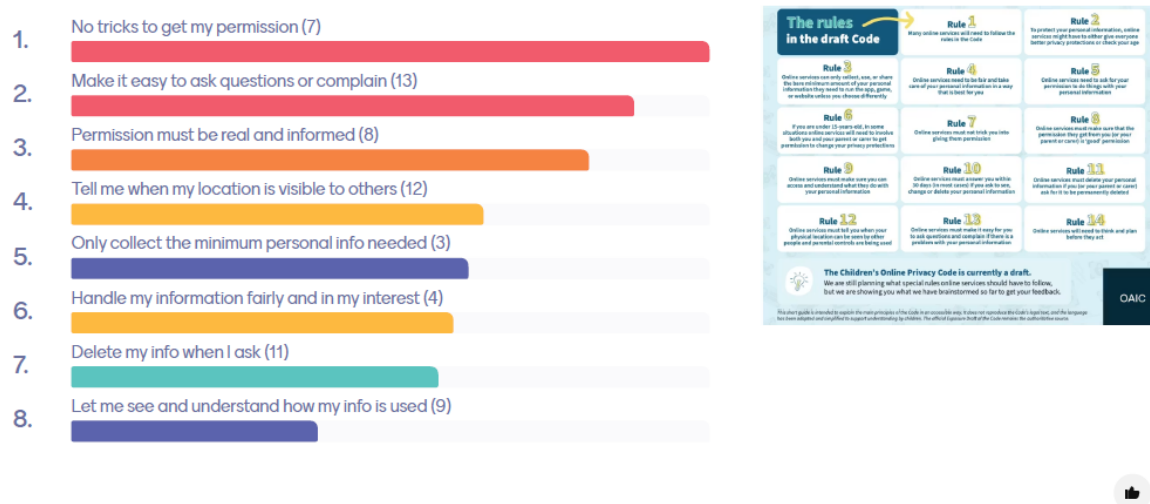


Chart 11: How might your online experience change with the introduction of the Rules? (pick up to 3)

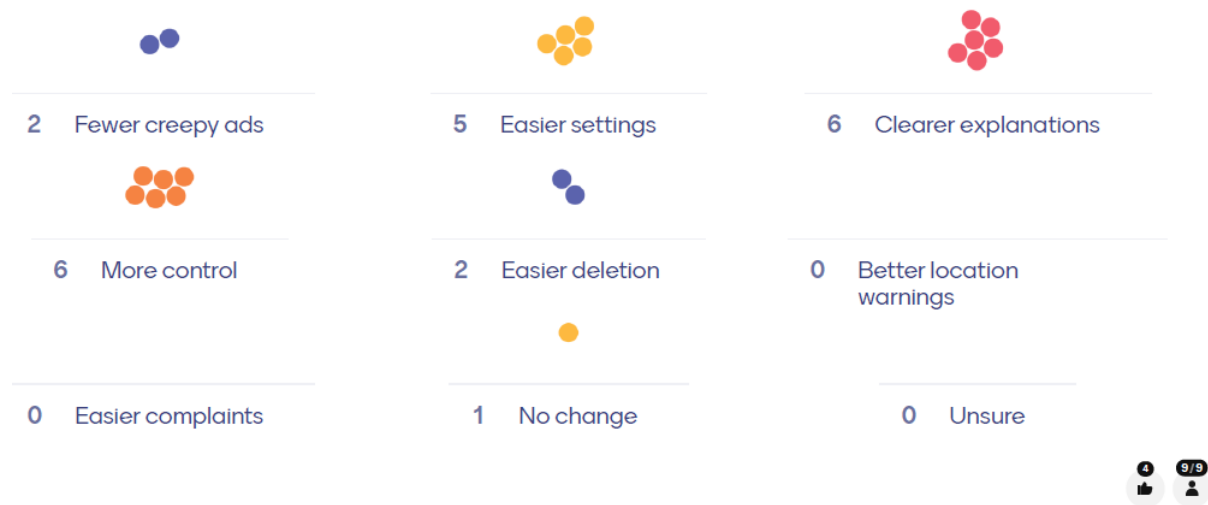


Chart 12: What's one thing the Code must get right to make your life online safer and more enjoyable?

