Life After the Social Media Ban for Under-16s

How the Australian Government's decision will really impact teens.

Presented by DigiChek

EXECUTIVE SUMMARY

What does our new data show?

DigiChek's national survey on the upcoming social media restrictions for under-16s reveals a public that strongly supports protecting children online yet remains sceptical about blanket bans and uneasy about intrusive age checks. Most respondents expect teens to route around restrictions unless platforms deploy practical, privacy-conscious measures that make safer services the easiest option. Our findings point to a clear path forward: empower platforms to implement creator-side content flagging and adopt privacy-first age assurance that does not harvest documents or biometrics.

Five Takeaways At A Glance

1. Awareness is already high. 62% of respondents knew about the coming under-16 rules before taking the survey.

2. Workarounds are expected. 58% believe the restrictions will not stop under-16s using social media.

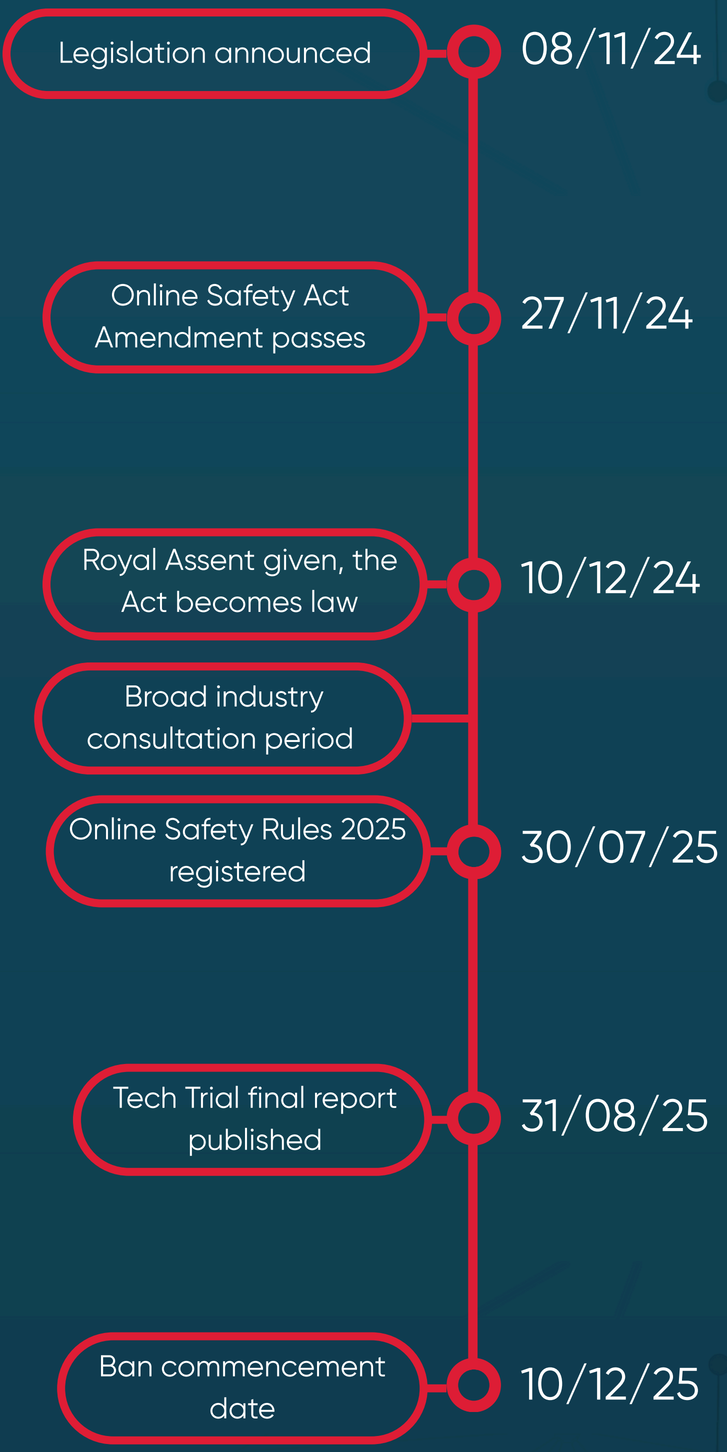
3. Privacy is the flashpoint. 70% worry about sharing personal data online, with heightened concerns about ID uploads and face scans.

4. Short-form video is the pressure point. TikTok is the most used platform among under-16s in our sample; video games and unrestricted messaging apps are the top expected alternatives if access is restricted.

5. Low-friction beats high-intrusion. Self-attestation and parent/guardian approval are rated higher than document upload or AI face scans despite government rejection; third-party verification is acceptable to consumers only if it is quick and low-data.

Why This Matters Now

The federal Social Media Minimum Age framework is due to take effect on 10 December 2025, with platforms required to detect and delete under 16 accounts, implement ways to confirm age of new accounts and provide age confirmation processes for those appealing inappropriate deletion, with eSafety registering new industry codes to limit children's exposure to pornographic and high-impact material. This creates both urgency and opportunity for solutions that protect kids without over-collecting their data.



Legislation announced 08/11/24

Online Safety Act Amendment passes 27/11/24

Royal Assent given, the Act becomes law 10/12/24

Broad industry consultation period

Online Safety Rules 2025 registered 30/07/25

Tech Trial final report published 31/08/25

Ban commencement date 10/12/25

DigiChek's Position

Australia needs **safety with privacy,** not a race to the bottom of what's easiest to implement. We recommend that the government and platforms combine (a) regulated platform-side and creator-side content flagging, and (b) **privacy-by-design age assurance** that keeps personal information off platforms altogether. DigiChek's approach stores no documents or biometrics and returns only an age result to the platform, because we began our development from a human, privacy-first approach.

How Was This Research Conducted?

Survey Design and Fieldwork

DigiChek conducted an online survey titled "Life After the Social Media Ban for Under-16s". Responses were anonymised at source. Quotes used in this report remain anonymous.

The instrument measured awareness of the under-16 restrictions, attitudes to enforcement, acceptance of verification methods, likely workarounds, and perceived benefits and harms of reduced social media access.

Duration

03/09/25 - 24/10/25

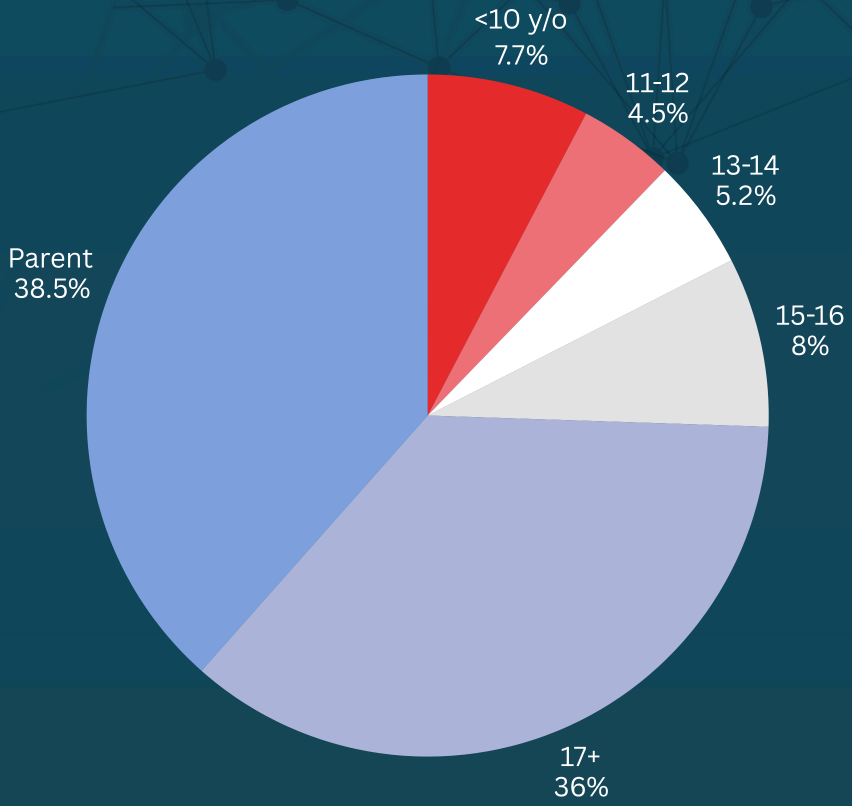
Sample Size

286

Who Took Part?

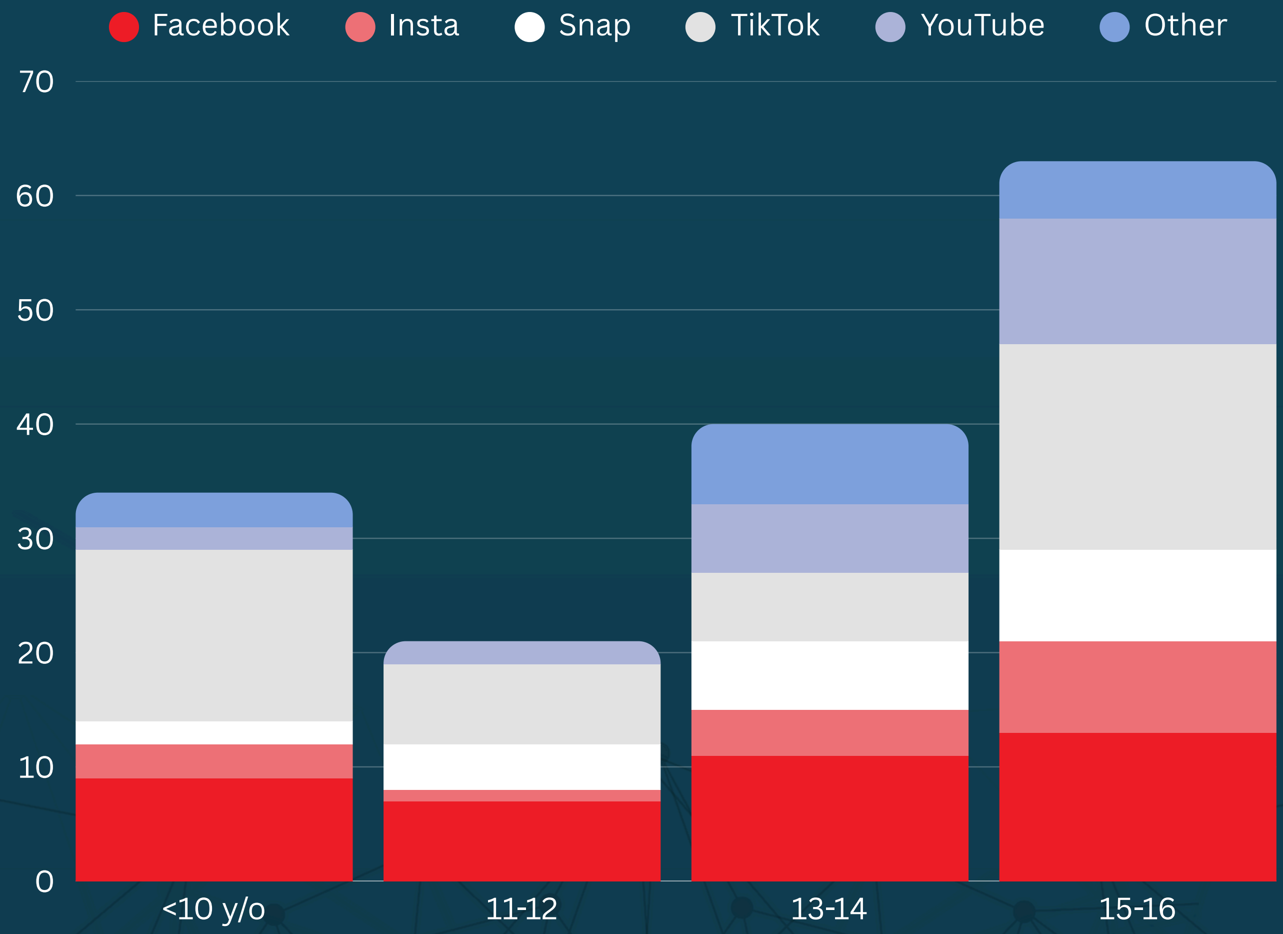
- Demographics: 73% of respondents were either parents or aged 17+; 27% were under 16. The gender split was 54% male, 42% female, 4% other.

- Usage patterns: Most respondents use social media several times a day. Facebook is most used overall among older respondents. TikTok is most popular among under-16s, with YouTube third across age groups. Messaging: WhatsApp 38%, Facebook Messenger 26%, SMS 17%.



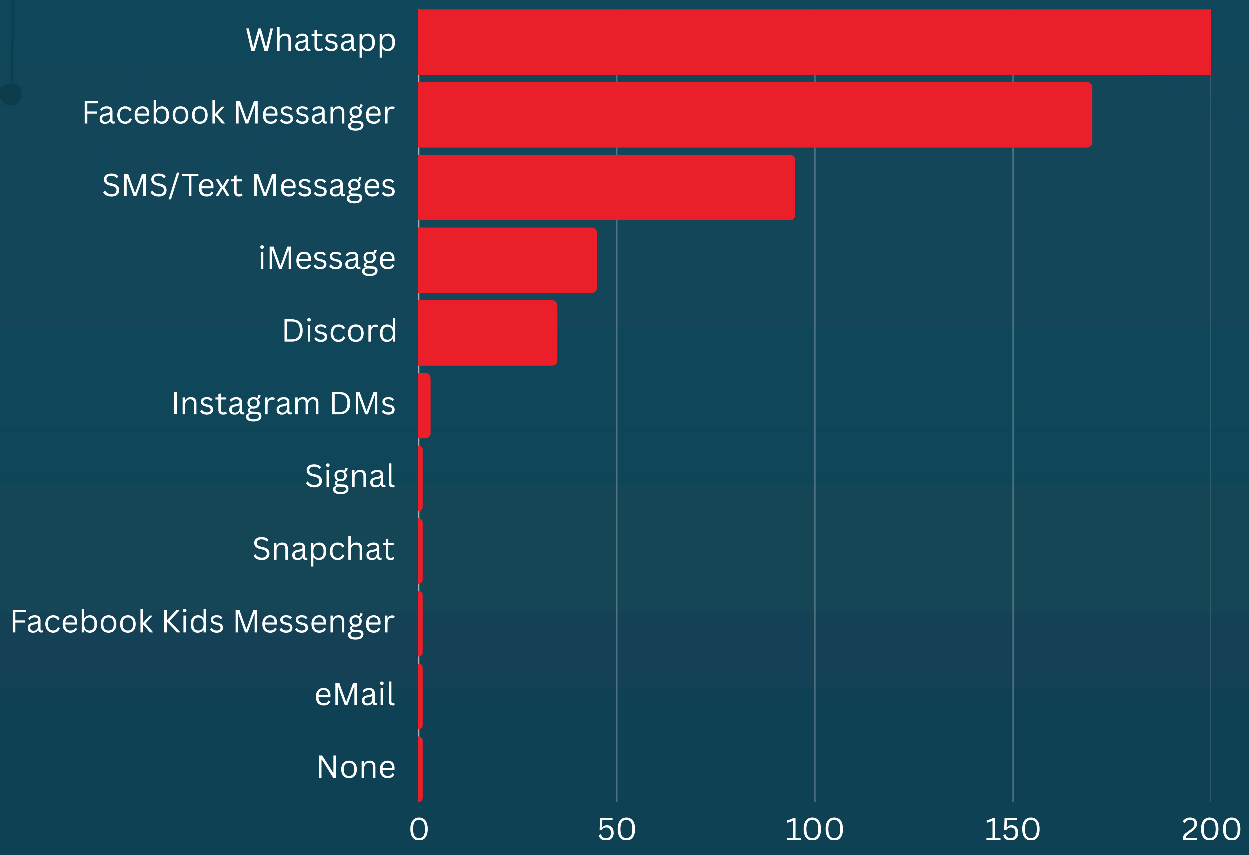
Respondent Age Groups

Preferred Social Platforms



Data sources: DigilChek Survey Insights, 2025 (internal analysis).

PREFERRED MESSENGER APP



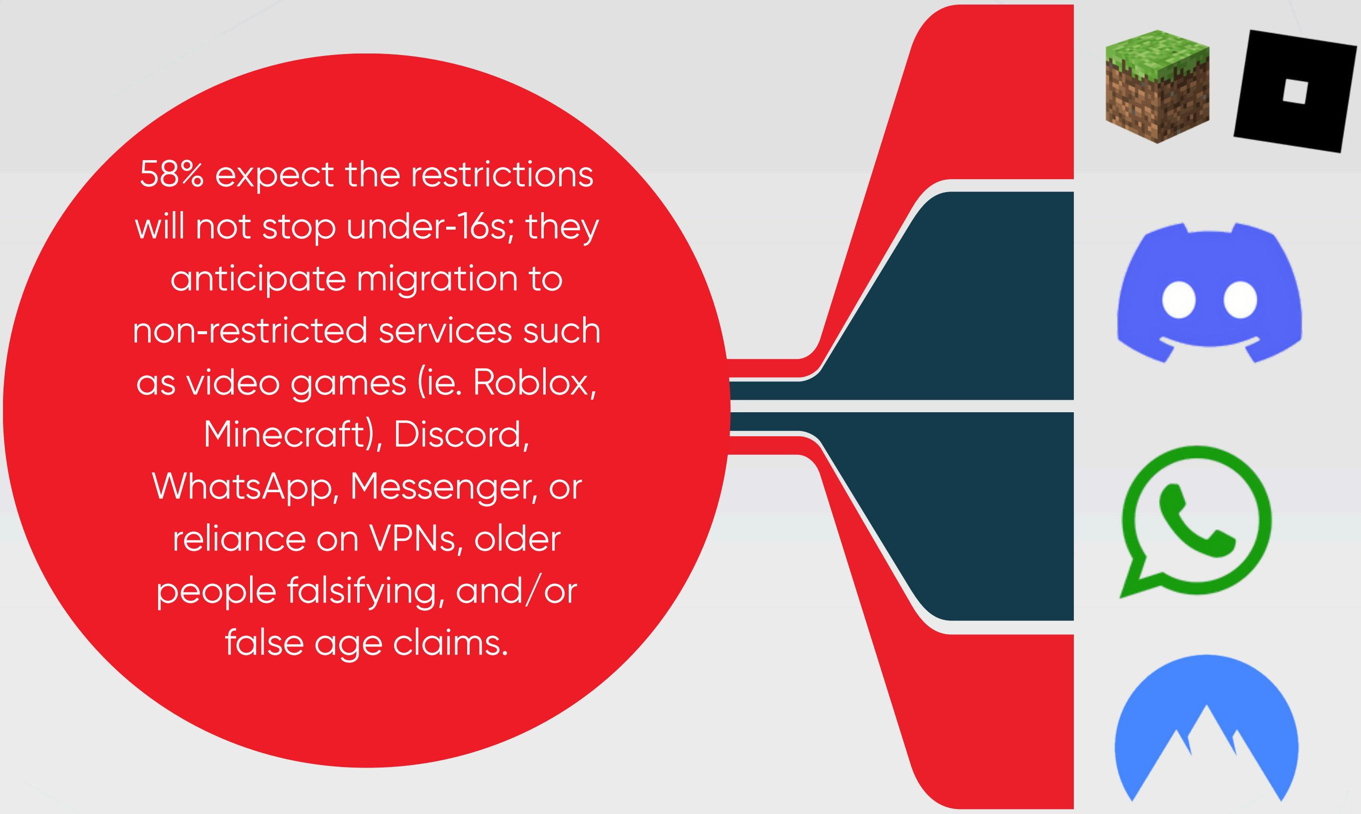
Data sources: DigilChek Survey Insights, 2025 (internal analysis).

Study Limitations

- The survey sample includes both under-16s and adults; results reflect mixed perspectives.
- As with all self-reported measures, stated intentions and actual behaviour can diverge, especially in fast-changing online environments.
- Platform policy specifics were still being finalised at the time of writing, which may shift some respondent expectations.

What Do Australians Think Will Happen After the Ban?

Expectation: Switching, not stopping



58% expect the restrictions will not stop under-16s; they anticipate migration to non-restricted services such as video games (ie. Roblox, Minecraft), Discord, WhatsApp, Messenger, or reliance on VPNs, older people falsifying, and/or false age claims.

Perceived Positives and Negatives

- **Perceived positives:** better mental health, more time for sport and hobbies, and increased in-person social connection.

- **Perceived negatives:** loss of online communities and distance friendships; fear of increased isolation for geographically dispersed or niche-interest teens. Particularly, vulnerable demographics like LGBTQ+, foster children, or abuse victims will be disproportionately affected by losing digital communities.

How do Australians feel about age checks?

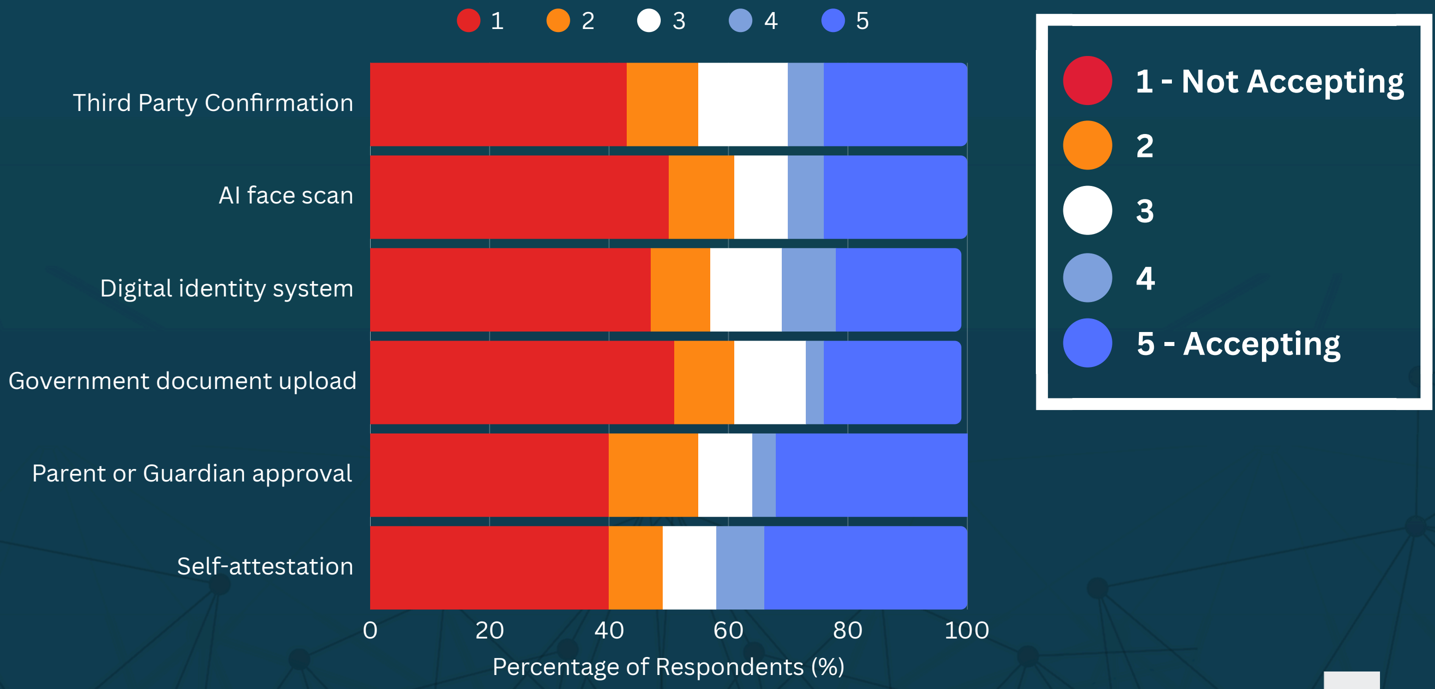
The privacy line

70% report privacy worries about sharing personal data online. Concerns centre on ID uploads, biometric face scans and uncertainty about how data is stored and who can access it.

Trust differentials matter: respondents show mixed acceptance for digital ID and third-party verification when accompanied by transparent, minimal-data processes; low acceptance for face scans and government-run uploads.

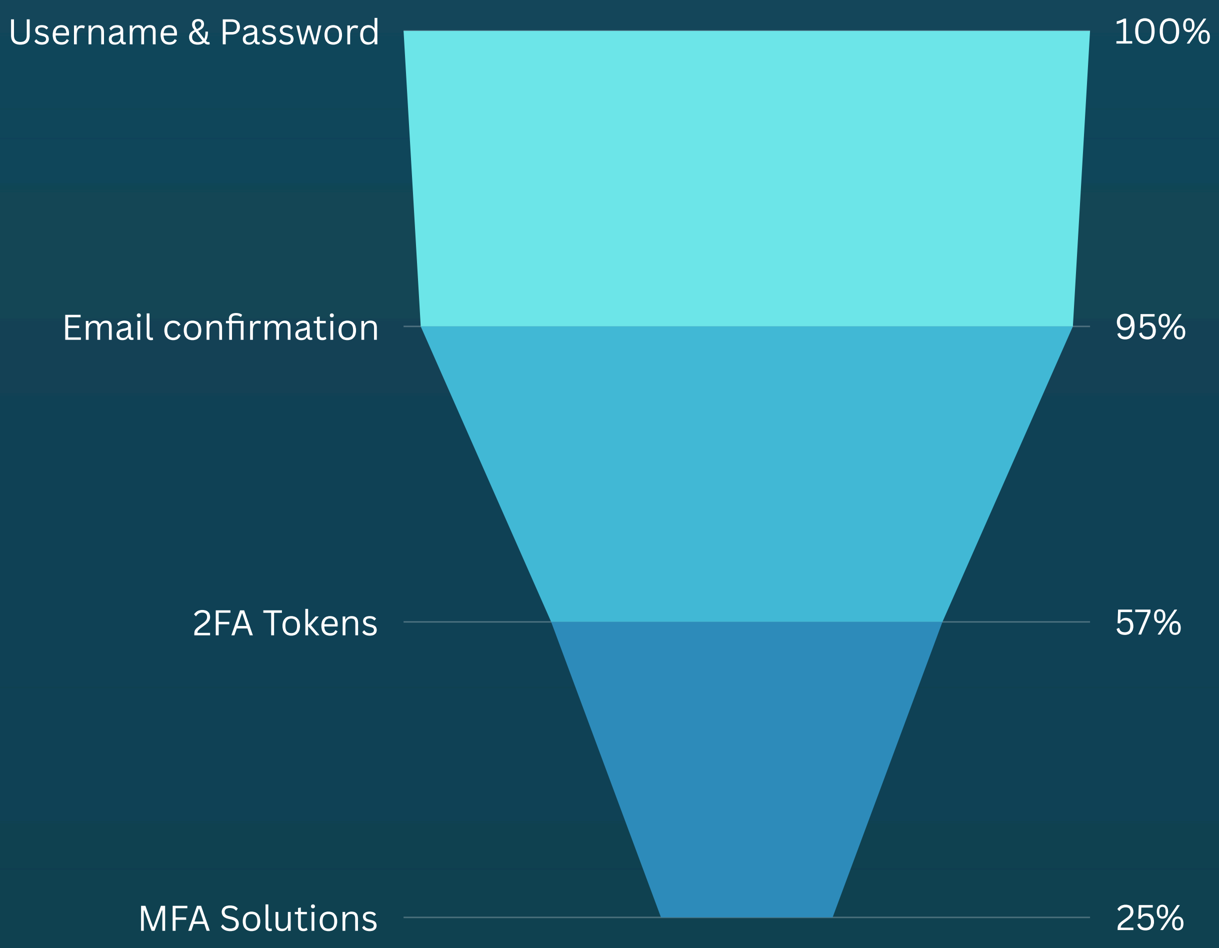
Under the regulatory guidance, self-declaration on its own is not sufficient for regulated contexts. However, by instead using age and identity confirmation tools like DigiChek Keys, users can actually control their online identity while complying with regulations and using platforms as allowed.

Acceptance of age verification methods



Ease and speed are decisive

Respondents emphasise the need for fast, low-friction verification at sign-up and login. Participants indicated they will resist or abandon multi-step processes that add minutes of friction or require repeated document submission. This is already being experienced by providers of 2FA tokens, and will only get worse when more steps are added to the process.



Representative comments

"If it takes more than a minute I'm out."
- Young person, WA

"I don't trust platforms with my ID, but I don't want my kids on TikTok either."
- Parent, NSW

"This legislation is an invasion of our civil liberties and is evil. It's not about keeping young people safe — parents are the ones to do that."
- Parent, QLD

"It would stop me from accessing educational information that school doesn't provide."
- Student, VIC

"Please don't make me upload my face to a random website. That feels worse."
- Student, NSW

"I do not want digital ID. Mum can help keep me safe online by knowing what I am watching."
- Student, VIC

"Taking away social isn't the same thing as giving me friends in real life".
- Student, QLD

"It should be up to the parents, not the government. They should fix the housing crisis, not social media."
- Student, QLD

"I get why they want to protect kids, but they'll just move to apps that aren't blocked".
- Parent, VIC

"What if a hacker hacks the app and steals the information?"
- Student, QLD

"Use a VPN and bypass it. I'm not doxxing myself online."
- Student, VIC

The Policy and Industry backdrop

What will change by December 2025?

The **Social Media Minimum Age** framework requires platforms to take **reasonable steps** to prevent under-16s from holding accounts by **10 December 2025.** The eSafety Commissioner is leading implementation and has registered six industry codes governing app stores, social media feeds, messaging features, equipment providers, and relevant electronic services.

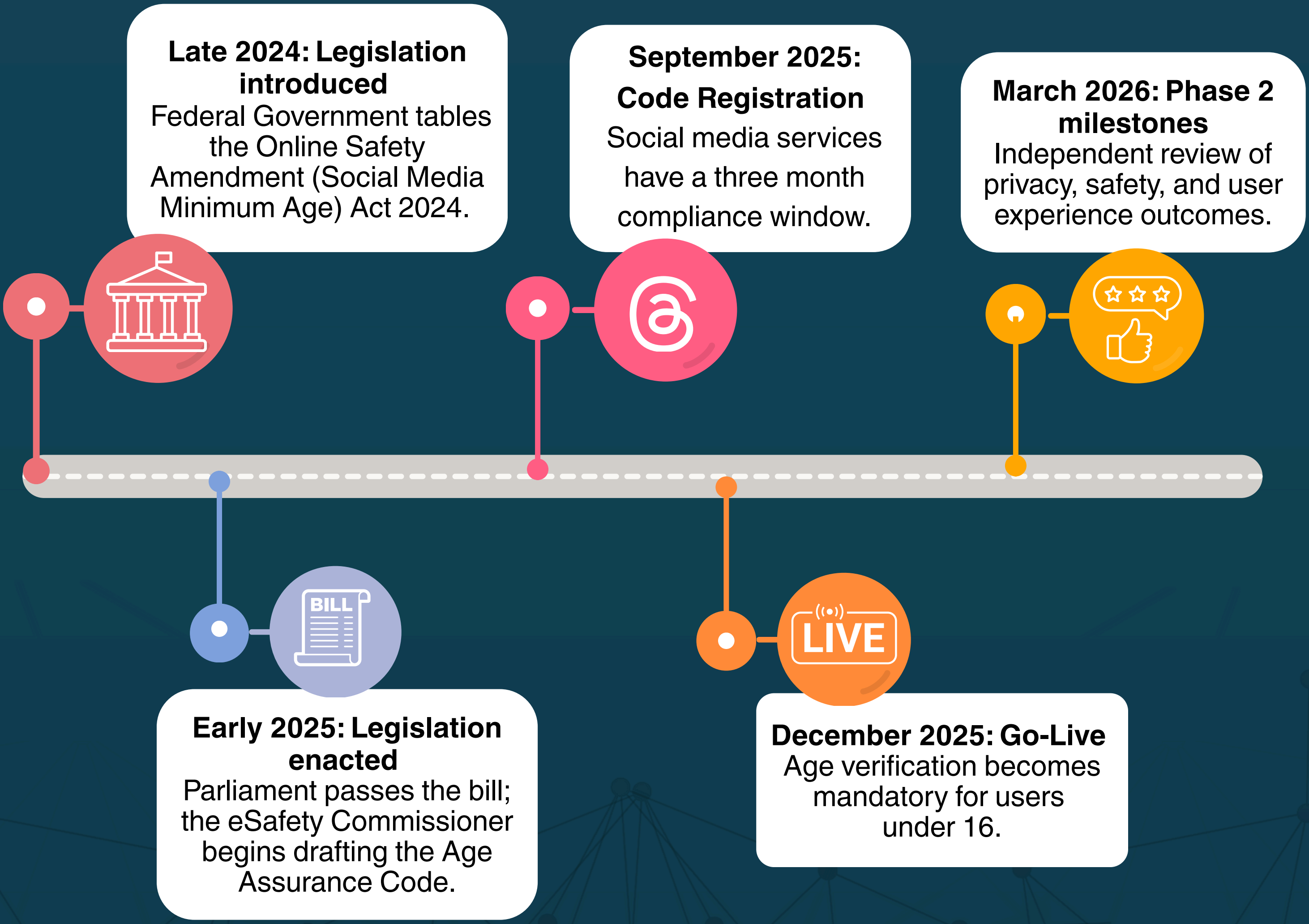
In parallel, **more complex age-checks** for online pornography and other high-impact content commence in **two phases** from **December 2025** to **March 2026**, increasing the demand for effective, privacy-protective age assurance.
In addition, **all search engines** will be required to use some form of age assurance technology on users or **face hefty fines**.

Platforms' stance and compliance planning

Major platforms have indicated they will comply with the new under-16 requirements while warning of enforcement challenges and potential displacement to less moderated spaces.

Why privacy incidents matter to teens and schools

Australia's higher-education and public sectors have experienced recent cyber incidents, reinforcing community sensitivity to the collection and storage of personal data about young people.



Late 2024: Legislation introduced
Federal Government tables the Online Safety Amendment (Social Media Minimum Age) Act 2024.

Early 2025: Legislation enacted
Parliament passes the bill; the eSafety Commissioner begins drafting the Age Assurance Code.

September 2025: Code Registration
Social media services have a three month compliance window.

December 2025: Go-Live
Age verification becomes mandatory for users under 16.

March 2026: Phase 2 milestones
Independent review of privacy, safety, and user experience outcomes.

What does the evidence say about enforcement risk?

The substitution problem

Our data suggests under-16s will substitute into messaging apps, video platforms, online game chats, and private communities if access to mainstream social media is restricted. This aligns with international experience: without friction-balanced design and creator-side flagging, bans can redirect rather than reduce harm exposure.

Recommendation 1:

Adopt **at-login and on-demand age checks** that return only an age decision, not identity data. Keep the checks **one-time or low-frequency** with reusable credentials to minimise friction, with strong appeal processes for false flags.

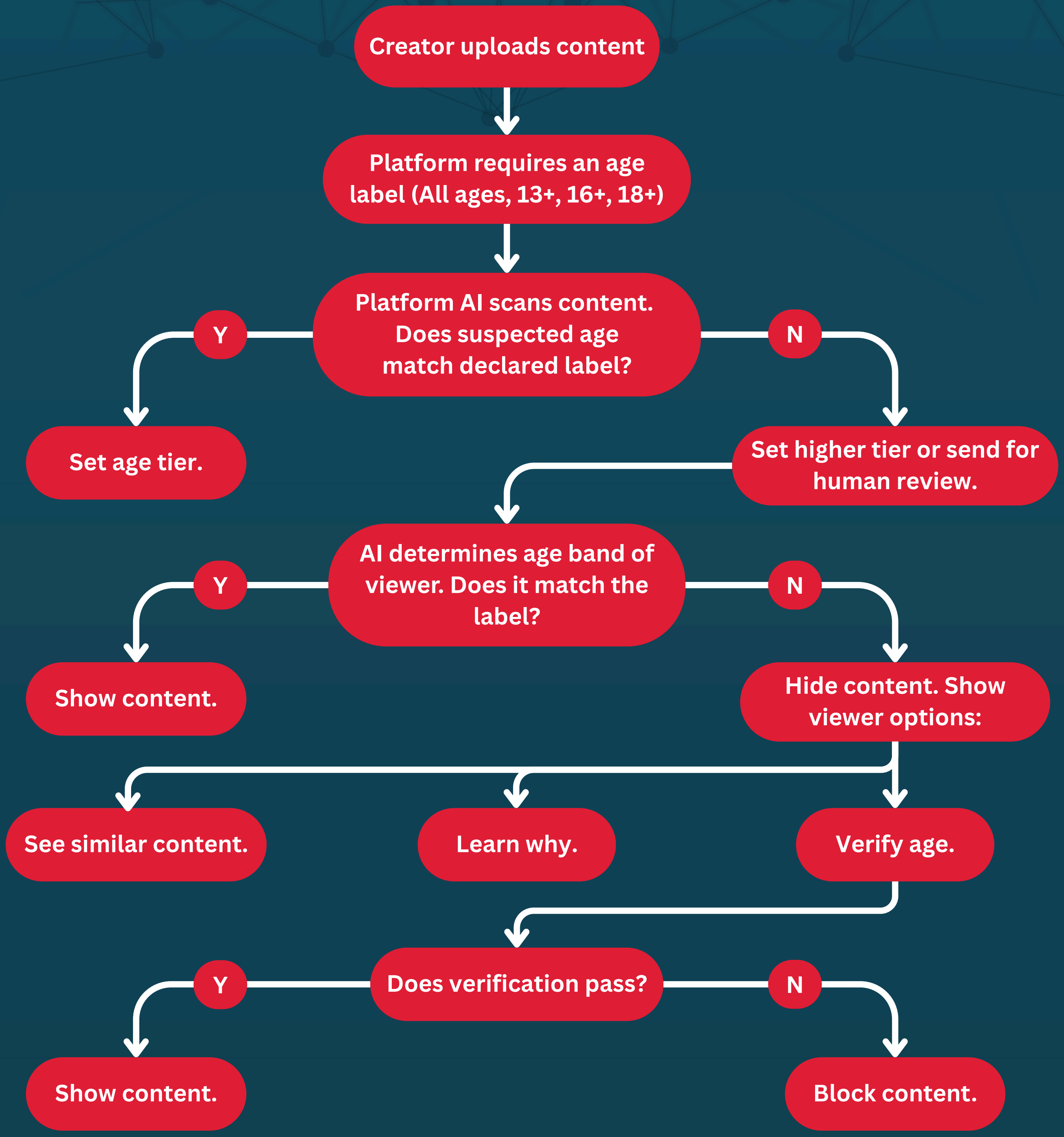
Recommendation 2:

Prefer **third-party**, minimum-data age assurance where platforms receive **only a Yes/No or age range result** and **do not** gain access to or store documents, biometrics, or government identifiers.

Recommendation 3:

Target **content pathways**, not just account age. Implement **mandatory creator-side content flagging** across major platforms, supported by platform algorithms that respect the flagging, so that **potentially harmful content is age-gated** wherever it appears.

Creator-side Content Flagging



Creator uploads content

Platform requires an age label (All ages, 13+, 16+, 18+)

Platform AI scans content. Does suspected age match declared label?

Y

N

Set age tier.

Set higher tier or send for human review.

AI determines age band of viewer. Does it match the label?

Y

N

Show content.

Hide content. Show viewer options:

See similar content.

Learn why.

Verify age.

Does verification pass?

Y

N

Show content.

Block content.

Public Expectations

Parents in our survey support stronger protections yet consistently reject data-hungry enforcement. Respondents voiced discomfort with document uploads and face scans. This aligns with national policy shifts that emphasise risk-proportionate and privacy-preserving age assurance rather than maximal data capture.

How DigiChek works

DigiChek enables age assurance with no document or biometric storage by platforms. Age confirmation occurs with trusted, trained, and independent verifiers for adults, and through educational institutions for students. Once verified, DigiChek receives only the user's name, DOB, and place of birth, and outputs a user-controlled credential, a DigiChek Key, that is never transmitted or stored outside DigiChek. Platforms ask a question about age and receive only a yes/no answer.

Data minimisation: DigiChek stores only name, date of birth, and place of birth. It does not collect government credentials, documents or biometrics.

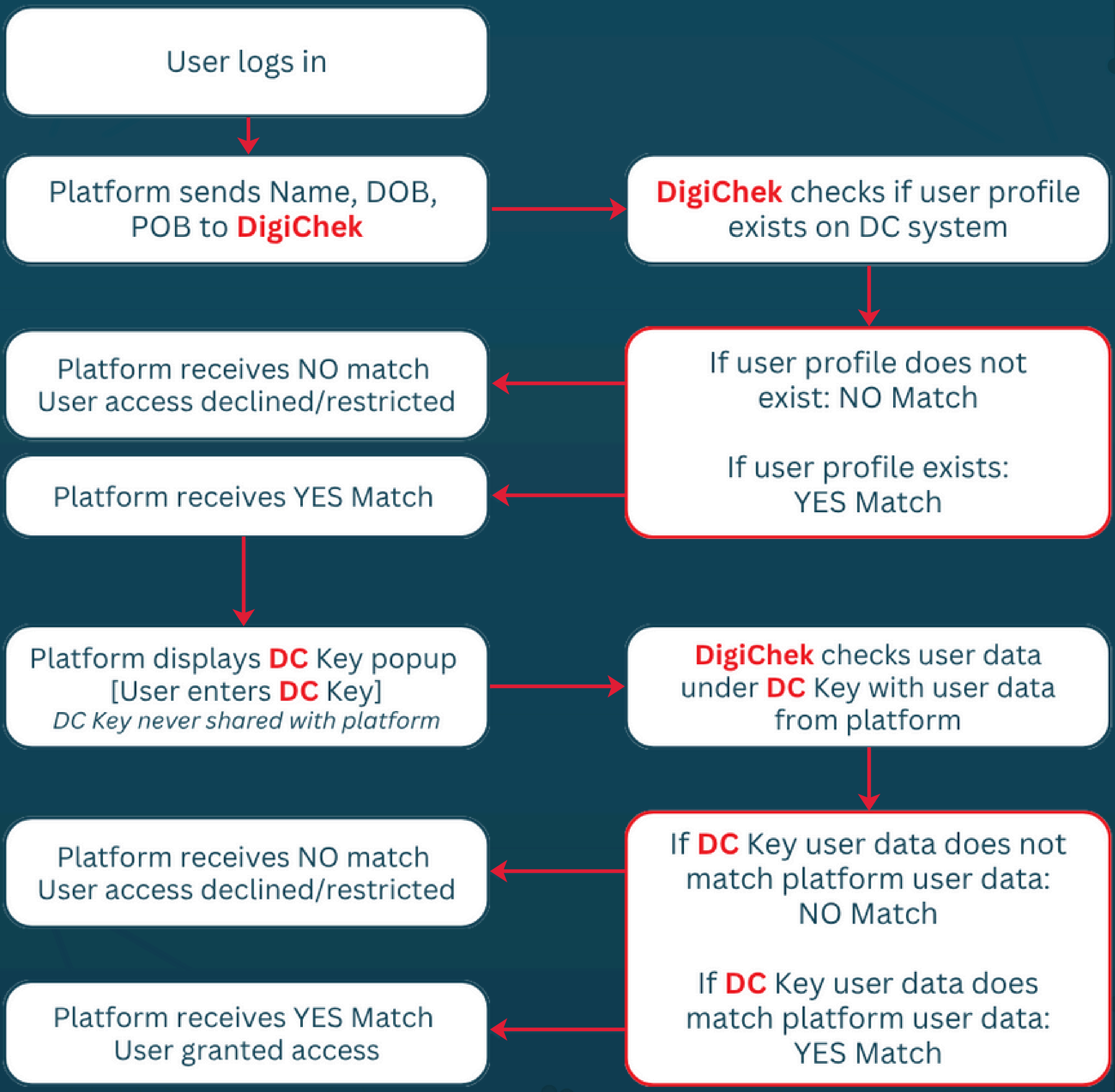
Privacy by design: Querying organisations receive only the age assurance result, not the underlying data, and exact ages can be suppressed in favour of over/under decisions.

Security: No centralised document store. Adults' credential checks remain with the verifying third parties. Children's data is retained by their educational institution; zero additional documents are required.

Standards alignment: Aligns with ISO 27566-1:2025 principles and international best practice.

Provenance: Acceptance testing shows cross-browser compatibility and confirms that no personal information is transmitted during verification.

The DigiChek System



User logs in

Platform sends Name, DOB, POB to **DigiChek**

DigiChek checks if user profile exists on DC system

If user profile does not exist: NO Match

If user profile exists: YES Match

Platform receives NO match
User access declined/restricted

Platform receives YES Match

Platform displays **DC** Key popup
[User enters **DC** Key]
DC Key never shared with platform

DigiChek checks user data under **DC** Key with user data from platform

If **DC** Key user data does not match platform user data: NO Match

If **DC** Key user data does match platform user data: YES Match

Platform receives NO match
User access declined/restricted

Platform receives YES Match
User granted access

DigiChek's policy recommendations for December 2025

1 **Adopt DC Keys as the default for age assurance and login confirmation across platforms.** Once verified, a user is confirmed at every login without revalidation, and the same DC Key will work on every participating platform and service.

2 **Use DC Keys as a password replacement that lowers friction and lifts security.** They remove the need for 2FA/MFA prompts with no change to platform business models or login flow. Simultaneously, they increase security by ensuring only the user - not the platform or a data broker - knows the DC Key.

3 **Set privacy floors for age assurance.** Prohibit routine document or biometric collection by platforms and require third-party checks that return only an age decision, with published test results and retention details.

4 **Prefer at-login confirmation over scheduled rechecks.** Confirmation happens seamlessly with the DC Key at sign-in, and users should experience minimal UI friction while maximising digital safety.

5 **Measure outcomes and improve continuously.** Track exposure reduction, false-positive rates, provide clear appeal paths and appeal outcome report, average verification time, and login confirmation success, and commission periodic independent audits.

How to use these findings

Look beyond the headline. Avoid assuming teens will be offline entirely. The data indicates likely migration to other, less secure services unless content-level controls improve.

Keep privacy central. Concerns about data misuse are **significant.** Consider this alongside recent sector breaches and evolving privacy reforms.

Scrutinise verification methods. Which methods are being used, what data is collected, where it is stored, and how false positives will be appealed all matter for community trust.

Examine creator-side flagging. Are uploaders traceable and required to classify content? And how will AI support and enforce those classifications across features like Reels, Shorts and Stories?

Key Takeaways

01

SUBSTITUTION

Under 16s will migrate to messaging apps, gaming chats, and private comunities rather than go offine entirely

02

PRIVACY ANXIETY IS HIGH

Most respondents fear identity theft or data misuse if age verification requires personal documents or biometrics.

03

PREFERENCE FOR INDEPENDENT VERIFICATION

The majority favoured third-party, privacy-preserving systems over government-run or platform-run checks.

04

EMOTIONAL AND SOCIAL IMPACT

Respondents predict loss of social connection as the top negative outcome, more than boredom or reduced screen time.

05

POTENTIAL SILVER LININGS

Some see the benefits with more free time, less bullying and more in person interactions. Respondents balanced frustration with hope for healthier online habits.

> “Personally, I’d like to be as anonymous and hard to track as possible, but still be able to prove my age. I don’t trust platforms with my ID.”
>
> By: Young Adult (17+)

> “Stop trying to ban and start teaching the kids to use social media responsibly.
> Education beats restriction.”
>
> By: Parent

How to talk to under-16s about the changes

START WITH RESPECT AND FACTS

It is a delay, not a criminalisation of teens. Explain what will change on platforms, what alternatives remain, and what your school's policies are likely to be.

EMPHASISE WELLBEING WITHOUT SHAME

Discuss sleep, attention, social comparison, and online conflict in practical terms. Help young people plan healthier routines that still include digital connection.

PREPARE FOR PLATFORM SHIFTS

Expect teens to move towards messaging apps, Discord, and/or gaming platforms. Reinforce privacy settings, reporting tools, and community guidelines in those spaces too.

AGREE ON CLEAR FAMILY OR SCHOOL NORMS

Co-write a media plan: times, places, and exceptions. Focus on consistency, not surveillance.

TALK ABOUT PRIVACY LIKE A LIFE SKILL

Explain why uploading documents or face scans to random sites can be risky. Prefer solutions where the platform sees only an age result, not personal data.

KNOW THE SUPPORT PATHS

Save the eSafety resources and school contacts. Encourage help-seeking if online harms occur.

Endnotes

- Department of Infrastructure, Transport, Regional Development, Communications and the Arts. “Social media minimum age.” Accessed October 30, 2025. https://www.infrastructure.gov.au/media-communications/internet/online-safety/social-media-minimum-age

- eSafety Commissioner. “Industry codes and standards.” Updated September 9, 2025. https://www.esafety.gov.au/industry/codes

- eSafety Commissioner. “Social media age restrictions: find out the facts about the ban or delay.” Accessed October 30, 2025. https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions

- The Guardian. “Australians will have to verify their age to watch pornography from December.” September 13, 2025. https://www.theguardian.com/australia-news/2025/sep/13/australians-will-verify-age-photo-id-facial-recognition-to-watch-pornography-from-december

- Reuters. “Meta, TikTok and Snap say they oppose Australia’s youth social media ban but will comply with it.” October 28, 2025. https://www.reuters.com/business/media-telecom/meta-tiktok-snap-say-they-oppose-australias-youth-social-media-ban-will-comply-2025-10-28/

- ABC News. “University of Western Australia suffers major data breach.” August 11, 2025. https://www.abc.net.au/news/2025-08-11/university-of-western-australia-uwa-suffers-major-data-breach/105636074

- Western Sydney University. “Cyber Incident – Public Notification 23 October 2025.” October 23, 2025. https://www.westernsydney.edu.au/news/cyber-details/october-23-202

- Office of the Australian Information Commissioner. “Children’s Online Privacy Code: children’s consultation report.” October 13, 2025. https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/childrens-online-privacy-code-childrens-consultation-report

Appendix A: One-page handout for schools and parents

Talking with teens about the social media changes

- Acknowledge feelings. It is normal to feel frustrated or anxious about changes.
- Explain the what and why. Focus on safety, not punishment. Clarify which features may change and what will remain.
- Co-design a plan. Set times and contexts for online time, gaming, and messaging that work for everyone.
- Strengthen safety basics. Privacy settings, reporting, blocking, and when to ask for help.
- Choose privacy-respecting tools. Prefer age assurance that shares only an age result with platforms and stores the minimum data.
- Before the deadline arrives, set up alternative communication channels for any online relationships the child wants to maintain.
- If the child has existing social profiles, download all existing information and photos to ensure nothing is lost upon the ban commencing.

Useful Links

- eSafety Commissioner: https://www.esafety.gov.au/young-people
- School wellbeing team: [insert your local contacts]
- State helplines: https://headspace.org.au/ | https://kidshelpline.com.au/

Appendix B: Source Notes

- All statistics in the body of this report are drawn from DigiChek's 2025 anonymised survey data and internal analysis. Source data can be provided upon request.

- Quotations are verbatim from anonymised respondent comments.

- Policy context and timelines reflect publicly available sources listed in Endnotes 1–8 at time of writing.