2025.12.09.1

RESIST KIT

GUIDE

EMPOWERING PARENTS

Teach, Don’t Tether

A practical parent guide to protecting kids online - without feeding Digital ID systems From December 2025, the Australian Government has announced plans to ban under-16s from using social media unless their age can be verified.

The legislation states that Digital ID is not mandatory, but age-assurance systems are the mechanism by which children and adults will increasingly be asked to “prove” who they are online: age assurance obligations are the gateway to Digital ID.

The Government has specified that social platforms will be required to use approved age-assurance methods.

1. **Biometric data** – a face scan of the user to estimate age.
2. **Physical ID** – verifying age by checking your ID (licence, passport, Medicare card) supplied to and approved through a third-party provider.
3. **Inference data** – using information already held about you, such as how long you’ve had your account, your stored birth date, or what Google/Apple know from your browser or device account.

None of these methods is foolproof, so platforms are expected to use a mix.

This guide helps parents stay compliant without unnecessarily submitting their children’s personal data into developing age-verification systems.

1. What the law requires — in plain English

- Platforms must block accounts for children under 16 unless an approved age-assurance method is used.
- Providers may offer Digital ID as the easiest verification route, but the law does not require families to use Digital ID.
- Parents must be able to consent to accounts for 13-15 year olds if the platform permits them.
- The government has stated that age verification must be “privacy-preserving,” but specific technical standards are still emerging.
- No requirement exists for parents to upload driver’s licences, birth certificates, or other identity documents directly to social media companies.
- Minors & consent: In Australia, anyone under 18 is a minor and generally cannot enter into binding contracts. The collection of biometric data (such as face scans for age verification) involves contractual terms and the handling of sensitive personal information, meaning valid parental consent is legally required for minors.

Get more resources & kit here: **www.MyResistKit.com**

ALIGNED COUNCIL OF AUSTRALIA

RCR .media

EMPOWERING PARENTS
Continued

GUIDE

2. Practical ways to comply without Digital ID

Instead of connecting your child to an identity system, use device-level, home-network, or parent-controlled tools:

A. Device & App Store Settings

- Turn on Apple Screen Time or Google Family Link to limit app installation by age rating.
- Block social media apps on the device itself.
- Require parent approval for all app downloads.
- Get or move your child to an un-smart phone

B. Home Network Filters

- Use router-level filters (built into many home Wi-Fi systems).
- Options include:
  - DNS-based filters like CleanBrowsing or OpenDNS
  - Blocking social media domains on the router

C. Local Profiles, Not Cloud Profiles

- Create a local user profile on the device rather than signing a child into a cloud ecosystem with personal identifying details.

D. Family Agreements

Establish expectations and boundaries early:

- No private messaging with strangers
- Devices stay in shared spaces
- Inform children that any use of their biometrics requires parental consent
- Set daily time limits
- Parents can inspect devices at reasonable intervals
- Encourage children to report uncomfortable content immediately

3. Tips to reduce data exposure within age-assurance systems

If you must verify age:

- Choose methods that do not require ID documents (e.g., device-based age checks, parental consent forms).
- Avoid uploading biometric images (face scans) where possible.
- Decline optional “upgrade to Digital ID” prompts.
- Check what school systems are using.
- Do not reuse your verification method across platforms unless truly necessary.

4. What to watch for as the policy rolls out

These areas may change as regulations mature:

- What counts as a compliant age-assurance method (standards are still being finalised).
- Whether platforms begin to nudge users toward Digital ID as the default option, even though not required.
- How appeals or disputes about age verification are handled.
- What data verification providers may store, and for how long.

ACA will update parents as clear regulations are released.

5. Remember the Principle: Teach, Don’t Tether

The safest, most resilient approach is teaching children how to navigate the online world - not blocking them entirely, or tethering them to identity systems.

Privacy is a skill.
Boundaries are teachable.
Kids grow - databases don’t.

Get more resources & kit here: **www.MyResistKit.com**

ALIGNED COUNCIL OF AUSTRALIA

RCR .media