Victorian Child Online Safety Guide

Practical prevention steps for parents and carers

Parents Online Safety Hub • Victoria-based • Australia-focused

Built by Graeme (aka Jinglez).

Core principle: Prevention is better than cure.

This guide is designed for busy parents. It is not about fear. It is about simple, repeatable habits that reduce risk online and help kids feel safe enough to speak up early.

Version 1 • 17 Feb 2026

Start in 10 minutes

If you do nothing else, do these five steps today.

- **Set the correct age** on the device and the app/game account.
- **Make accounts private** and restrict who can message your child (Friends only).
- **Turn voice chat off by default** for younger kids (enable case-by-case).
- **Stop off-platform moves**: no Discord/Snap/WhatsApp invites without parent approval.
- **Shared charging**: devices charge overnight in a shared area (not bedrooms).

House rules that actually work

- Under 13: devices used in common areas as a default.
- Weekly calm check-in: “Anything weird online this week?”
- No secrets with adults online - ever. Surprises are okay; secrets are not.
- If something feels off, they won’t lose their device for telling you.

One sentence you can use

“If anyone asks you to keep something secret, move to another app, or send photos - you stop and tell me straight away.”

Online grooming: what it often looks like

Grooming usually starts small: friendliness, flattery, gifts or attention. It can slowly shift into secrecy, isolation, and sexual content. The pattern matters more than any single message.

Common warning signs

- Requests for secrecy: “Don’t tell your parents.”
- Pushing to move chats off the platform (Discord, Snap, WhatsApp).
- Gifts, in-game currency, skins, or “special” treatment.
- Boundary testing that becomes sexual or controlling.
- Requests for photos, video, or “proof” of trust.
- Questions about routines: school, times alone, where they live.
- Your child becomes unusually secretive, anxious, or defensive about devices.

Protective responses

- Stay calm. Thank your child for telling you.
- Screenshot usernames and messages (include dates/times where possible).
- Block and report inside the platform after you have captured evidence.
- Do not confront the person directly - protect evidence and reduce risk.

Device and platform basics (non-techy friendly)

You do not need to be an expert. You need a repeatable routine. Start with these four settings on every platform your child uses.

- **Privacy:** account set to Private.
- **Messaging:** Friends only.
- **Friend requests:** restrict or require approval.
- **Voice chat:** off by default for younger kids.

Monthly 5-minute check (set a reminder)

- Review the friends list together - remove strangers.
- Check privacy settings didn’t reset after app updates.
- Check purchase settings (in-app purchases).
- Revisit the rule: no off-platform invites without approval.

Gaming platforms: simple rules

- Keep chat on Friends only where possible.
- Disable DMs from non-friends.
- Teach kids: never share name, school, suburb, photos, or schedules.
- If they want to play with someone new: add in a supervised way, then review after.

Reporting (Victoria-based, national options)

If you suspect grooming, exploitation, or a serious online threat, use official pathways. Keep evidence first.

Immediate danger

Call 000 if a child is in immediate danger.

Where to report (common pathways)

- **Victoria Police** - report serious offences and immediate risks.
- **eSafety Commissioner** - help with online abuse, image-based abuse, and platform takedown pathways.
- **Australian Centre to Counter Child Exploitation (ACCCE, AFP)** - national reporting and coordination for child exploitation matters.

Evidence checklist

- Usernames, profile links (if available), and screenshots.
- Dates/times, platform name, and any account IDs.
- Any threats, requests for images, or attempts to move off-platform.
- If images are involved: do not share them with others. Use official reporting pathways.

Printable: Family Digital Safety Agreement

Use this as a starting point. Adjust to fit your family.

- We use **private accounts** and keep messaging to **friends only**.
- We do not move chats to other apps without parent approval.
- We do not share our real name, school, suburb, photos, or schedules with strangers.
- If anything feels weird, we tell a parent immediately and we won't be punished for speaking up.
- Devices charge overnight in a shared area.

Printable: 60-second safety check

- Is the account private?
- Who can message? (Friends only)
- Who can add friends? (Restricted)
- Is voice chat off by default?
- Any new "friends" we don't know in real life?

Want to help this stay free?

Support the project via GoFundMe: gofund.me/dbe68f536

Updates/subscription email: allthewaycarpentry@gmail.com