

PARENT QUICK SETUP CHECKLIST



The Chapter 7 sixty minutes, on one page. Do it in this order.

- ☐ Child account created inside Family Sharing (Apple) or Family Link (Google), with the REAL birthday
- ☐ Screen Time passcode or parent PIN set (not your phone unlock code)
- ☐ Ask to Buy / Google Play purchase approvals ON
- ☐ No bank card stored on any child account
- ☐ App permissions audited: camera, microphone, photos, contacts, location, per app
- ☐ Location per app: Never or While Using only
- ☐ Downtime scheduled; chargers out of ALL bedrooms tonight
- ☐ SafeSearch on and locked; web filter set for age
- ☐ Router DNS changed to 1.1.1.3 and 1.0.0.3 (or 208.67.222.123 and 208.67.220.123); router admin password changed
- ☐ Guest WiFi switched on for visitors and old devices
- ☐ Two factor authentication on the child's email first, then all accounts
- ☐ Platform family tool linked for every installed social and gaming app
- ☐ Said out loud while doing it: "I am closing doors that should never have been open, not spying on you"

Date: _____

MONTHLY PHONE SAFETY CHECKLIST



Ten minutes, child present, tone of maintenance. Same day each month.

- ☐ App list swiped through together: anything new gets explained by them, not interrogated by you
- ☐ Install and delete history glanced at (app store account history)
- ☐ Friends, followers, pending requests on TWO apps (rotate monthly): "who is this?" asked lightly
- ☐ Privacy, DM, and location settings still as agreed (updates reset things)
- ☐ Payments, subscriptions, and any game currency that arrived from outside the family
- ☐ Linked devices and active sessions on their main accounts
- ☐ Any VPN installed? A question, not a verdict
- ☐ Screen time report: what happens after 22:00?
- ☐ Family tool links still connected (TikTok, Meta, Snapchat, Discord, console)
- ☐ One open question, phone down: "Anything online lately that felt off, even slightly?"
- ☐ Phone handed back; something normal happens next

Date: _____

GAMING SAFETY CHECKLIST



- ☐ Every game checked against the seven mechanics: voice chat, text chat, friend requests, username, location clues, gifts, off platform movement
- ☐ Username contains no real name, birth year, school, or city
- ☐ Chat set to friends only (or off for under 10s) on every platform
- ☐ Friend requests: parent approval for under 13s
- ☐ Voice chat with strangers OFF; headset use in shared spaces for younger children
- ☐ Purchase approvals on; no stored card; gift currency from outside the family is always reported to a parent
- ☐ Discord server list audited out loud monthly: "what is this one?"
- ☐ Roblox: parent account linked, spending limit set, chat age band confirmed
- ☐ Consoles: communication settings per child, ask to buy on, activity reports arriving
- ☐ The moving rule taught: "new platform, new person, tell me first"
- ☐ The gift rule taught: "if anyone in a game gives you things or offers to, tell me"
- ☐ No livestreaming under 13; teen streams private, camera aware of background

Date: _____



SOCIAL MEDIA SAFETY CHECKLIST

The Chapter 4 lockdown. Contact first, location second, content third.

- ☐ Real birthday on every account (every protection keys off it)
- ☐ Private account on every platform; "suggest my account" off
- ☐ DMs: friends or contacts only, or off (TikTok, Instagram, Snapchat Contact Me, Discord requests, Reddit)
- ☐ Snap Map on Ghost Mode; WhatsApp Live Location off
- ☐ WhatsApp and Telegram group adds: My Contacts only
- ☐ Parent tool linked: Family Pairing, Meta supervision, Snapchat Family Center, Discord Family Center, YouTube supervision
- ☐ Content filters on: Restricted Mode, 13 plus or Limited Content, Snapchat restrictions, YouTube content level
- ☐ WhatsApp media visibility off; Instagram DM nudity protection confirmed on
- ☐ YouTube Shorts limit set (zero is an option)
- ☐ Two factor authentication on every account
- ☐ Follower lists reviewed monthly: the question is never the number, it is "who is this?"
- ☐ Anonymous apps: I suggest no for under 16s; random video chat: I suggest blocking it

Date: _____



AI SAFETY CHECKLIST

- ☐ Family photo audit done: no public posts with uniforms, school gates, full names, or birth dates
- ☐ Family accounts sharing child photos set to private
- ☐ School and sports club asked about their photo posting and consent policy
- ☐ Family code word chosen and taught (defeats voice clone scams); grandparents briefed
- ☐ The callback rule taught: any emergency call gets verified by phoning back on a known number
- ☐ AI companions: I suggest none under 13; teens' AI apps known and discussed
- ☐ Snapchat My AI disabled via Family Center if wanted; Fortnite AI chat setting checked
- ☐ The AI images script said once, calmly (Chapter 5): fakes can be made of anyone, fakes can be reported, the person who makes one is responsible
- ☐ Take It Down bookmarked: takeitdown.ncmec.org
- ☐ Homework rule set: AI can explain, the child writes, nothing personal typed into any AI

Date: _____



PRIVACY AND LOCATION CHECKLIST

- ☐ Per app location permissions: Never or While Using, every app, every device
- ☐ Find My / Family Link location sharing: family only, by open agreement, everyone knows
- ☐ Snap Map: Ghost Mode
- ☐ Photo access per app: Selected Photos, not full library
- ☐ Camera and microphone permissions: only apps with an obvious reason
- ☐ Contacts access: revoked from games and social apps that do not need it
- ☐ Cloud backup: on, and you know which account owns it
- ☐ Unknown tracker alerts: taken seriously, never dismissed as glitches
- ☐ Public profiles carry no school name, no full birth date, no home suburb
- ☐ The screenshot rule taught: if it appears on someone else's screen, they can keep it
- ☐ The deletion rule taught: deleted is a folder, not an ending; in a crisis, save before deleting

Date: _____



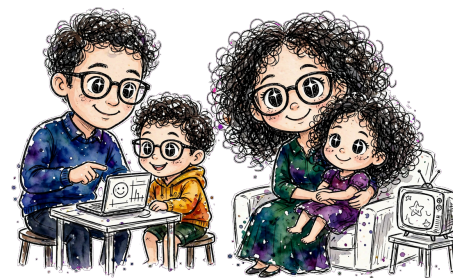
HOME SAFETY AND DEVICE INTEGRITY CHECKLIST

From Chapter 6. For devices that move between households or were set up by someone you have reason to distrust. If abuse is active: document, get advice, change nothing yet. Removal can alert.

- ☐ Does the other person repeatedly know things they could only know from private messages, conversations, or locations?
- ☐ Battery draining fast, device running warm, data spiking without explanation?
- ☐ Unfamiliar apps, or duplicate "system" looking apps?
- ☐ Settings changed that the child denies changing; a backup enabled that you never set up?
- ☐ Location on for apps with no reason; Find My or locator sharing with the wrong people?
- ☐ Unknown tracker alert on any phone in the household, ever?
- ☐ Logged in devices or active sessions you do not recognise on any account?
- ☐ Child's account inside a family plan organised by the person of concern?
- ☐ Device arrived as a gift, pre set up, or was handled alone by the person of concern?
- ☐ Child questioned after visits, or asked to install anything or share passwords?

One item alone can be innocent. A cluster, or one item plus the first, means: safe device, specialist advice (stopstalkerware.org), evidence first, then act, in the Chapter 6 order.

Date: _____



FAMILY DEVICE AGREEMENT

Print, discuss, adjust together, sign. Review each birthday. This is the parents' side and the household rules; the child's agreement follows.

Our family agrees:

- 1 Devices are looked after by the parents, the same way the front door is. Safety settings are set openly, never in secret.
- 2 Chargers live outside bedrooms overnight. Everyone's, including the adults'.
- 3 New apps get installed through approval, and every new app gets its settings done together on day one.
- 4 There is a short device check each month. It happens WITH you, not to you. It looks at safety areas (who can reach you, settings, unknown contacts), not your private conversations with friends.
- 5 Deeper checking only happens if there are serious warning signs, and you will be told what and why.
- 6 **The protection promise: you will not lose your phone or the internet for telling us about a problem. Reporting something is not punished.**
- 7 Mistakes get help first. Consequences, if any, are about behaviour, never about the telling.
- 8 Parents follow the rules too: we ask before posting photos of you, and we put our own phones down at meals.
- 9 Location is shared inside the family only, by agreement, and everyone knows it is on.
- 10 Every year this agreement loosens as trust and age grow. By eighteen, it is yours entirely.



FAMILY DEVICE AGREEMENT

Print, discuss, adjust together, sign. Review each birthday. This is the parents' side and the household rules; the child's agreement follows.

Our family agrees:

Signed (parent/s)

Date

Signed (parent/s)

Date

Discussed with

Date

Review each birthday

Date reviewed	What we changed together	Initials



CHILD ONLINE SAFETY AGREEMENT

The child's side. Read together. The child signs when they can explain each line in their own words.

I agree:

- 1** I use my real birthday on accounts, because the safety settings only work if it is true.
- 2** If anyone online asks me to keep a secret from my parents, that is the one thing I always tell them. The secret is the danger, not me.
- 3** Nobody may ask me for photos of my body. If anyone does, it is never my fault, and I tell my parents straight away.
- 4** If someone I met online asks me to move to a different app, I tell my parents before I move.
- 5** Gifts, game money, or offers from people online always get shown to my parents. I will not be in trouble and I will not have to give them back.



CHILD ONLINE SAFETY AGREEMENT

- 6 Before I send anything, I ask: would I be okay if the whole class saw this? Anything on someone else's screen can be kept.
- 7 If anyone threatens me, blackmails me, or says "or else," I tell my parents THAT DAY, even at 02:00, even if I made a mistake first.
- 8 If I see something scary or meant for adults, I can tell my parents. Seeing something is not the same as looking for it, and I will not be in trouble.
- 9 I do not share my passwords with anyone except my parents. Not even my best friend.
- 10 I know the family promise: telling never costs me my phone. So I tell.

In my own words, the one that matters most to me is

Signed (child)

Date

Signed (parent)

Date



EMERGENCY EVIDENCE CHECKLIST

From Chapter 11. Save BEFORE you block, delete, or clean anything.

- ☐ Offender's username, display name, and profile link
- ☐ Full conversation screenshots, from the very first message, times visible
- ☐ Platform names and where the contact started
- ☐ Phone numbers, emails, and other accounts they mentioned or moved to
- ☐ Payment demands and details; any payments already made
- ☐ Chat exports where the app offers them
- ☐ **THE EXCEPTION: never save, screenshot, or forward sexual images of any child. Capture URLs, usernames, and dates instead.**
- ☐ Block the offender's account only after saving. Do not delete your child's account, the profile or the messages.
- ☐ One dated folder, plus a second copy somewhere safe
- ☐ Case numbers and report references written down as you go

Date: _____

CONVERSATION STARTER CARDS



One card, one moment, no follow up interrogation. Full scripts live in Chapter 10.

5 to 7

What was the best thing you played today, show me how it works.

Did anyone talk to you inside a game this week?

What would you do if the screen showed something scary?

Tell me our secrets rule.

8 to 10

Anyone new you have been playing with lately?

Has anyone online ever asked you something that felt weird?

What is the meanest thing you have seen anyone do online?

If someone asked you to move to a different app, what would you do?

11 to 13

What is going around your grade's group chats at the moment?

Do people at your school ever ask each other for photos?

If something bad happened online tonight, who would you actually tell?

What would make it easier to tell me things?

14 to 17

Has anyone you know been hit by the sextortion scam?

What actually happens when a nude gets shared at your school?

Straight answer, zero consequences: anything on your phone you would want help with?

What is one thing adults get completely wrong about being online at your age?

GLOSSARY OF TERMS



Age assurance

methods platforms use to check or estimate a user's age, from typed birthdays (the least reliable) to ID checks and facial estimation.

Algorithm / the feed

the system that chooses what your child sees next.

CSAM

child sexual abuse material. The correct term; every image is evidence of a child being abused.

Cyberflashing

sending unsolicited sexual images.

DM

direct message; a private message inside an app.

Doxxing

publishing someone's private details (address, school, number) to invite harassment.

Deepfake

AI made image, video, or audio of a real person doing or saying something they never did.

End to end encryption

only the sender and receiver can read the messages; the platform generally cannot.

Family plan organiser

the account that controls a shared subscription or family group, and can often see members' activity or location.

Grooming

building a relationship with a child in order to abuse or exploit them. It can involve attention, flattery, gifts and secrets.

Loot box

a paid in game reward of unknown contents, with chance mechanics similar to gambling.

Metadata

data about data, such as when and where a photo was taken.

Nudification tool

software that fabricates a nude image from an ordinary clothed photo.

Parasocial relationship

a one way bond a child feels with a creator who does not know they exist.

Sextortion

blackmail using an intimate image, real or fabricated. In NCMEC and Thorn data, about 90% of victims in the financial sextortion cases analysed were boys aged 14 to 17.

Sharenting

parents oversharing children's photos and details online.

Stalkerware

hidden software that reports a device's messages, photos, location, and calls to another person.

Streaks

daily contact counters that can turn friendship into an obligation.

Take It Down

free anonymous NCMEC tool that helps remove a minor's intimate images from participating platforms. takeitdown.ncmec.org

Vault app

an app that hides photos or files, sometimes disguised as a calculator.

VPN

routes internet traffic through an encrypted tunnel; can protect privacy on public WiFi and can bypass home filters and age checks.

2FA / two factor authentication

a second code needed to log in. Codes are never read out to anyone.

CONDENSED RESOURCE DIRECTORY



The full directory with descriptions is Chapter 12. This is the fridge version.

CRISIS

Childline SA 116

SADAG 0800 567 567

SAPS 10111

Childline UK 0800 1111

US 988

AU Kids Helpline 1800 55 1800

Canada 9-8-8 and Kids Help Phone 1-800-668-6868

anywhere: findahelpline.com

IMAGE REMOVAL

takeitdown.ncmec.org (global, under 18, incl. AI)

Report Remove via childline.org.uk (UK)

needhelpline.ca (Canada)

REPORT EXPLOITATION

missingkids.org/gethelpline/cybertipline (global)

fpbhotline.org.za (SA)

inhope.org (find your country)

esafety.gov.au (AU)

cybertip.ca (Canada)

SA POLICE

10111 or Crime Stop 08600 10111; ask for the FCS Unit by name at your nearest station

GUIDANCE

esafety.gov.au/parents

nspcc.org.uk

internetmatters.org

commonsensemedia.org

FAMILY ABUSE AND STALKERWARE

stopstalkerware.org

nnedv.org

riseagainstdomesticviolence.co.za

SETUP

support.apple.com/en-us/105121

families.google/familylink

youtube.com/myfamily

familycenter.meta.com

WARNING SIGNS LIST



No single sign proves anything. A cluster, or one sign plus your gut, means look closer. The full table with first moves is in Chapter 2.

- | | |
|--|---|
| ☐ Sudden panic, dread, or secrecy attached to the phone | ☐ New contempt for girls or women, delivered as irony |
| ☐ A new friend, gift, or game currency you cannot explain | ☐ Sexual knowledge beyond their age |
| ☐ Apps appearing or vanishing overnight | ☐ Requests for money or gift cards with a thin story |
| ☐ Switching screens when you enter | ☐ Anyone asking the child for secrecy |
| ☐ Late night use plus wrecked mornings | ☐ Distress after gaming |
| ☐ Withdrawal from sport, friends, meals | ☐ A second phone or unfamiliar device |
| ☐ Covering arms or legs; unexplained injuries | ☐ Talk of meeting an online friend |
| ☐ Tightening food rules; guilt at meals | ☐ Jokes about disappearing that are not quite jokes (this one needs help now: see the crisis lines in Tool 13) |

Date: _____

FIRST 24 HOURS ACTION PLAN



The Chapter 11 flow, compressed. Immediate danger: 10111 first.

Hour 0 to 1: the child.

Say it before you understand everything: *"I am not angry with you. You are not in trouble. We fix this together, starting now."* Do not contact the offender. NCMEC says paying rarely stops sextortion, so get help before deciding about payment. Do not delete anything.

Hour 1 to 3: the evidence.

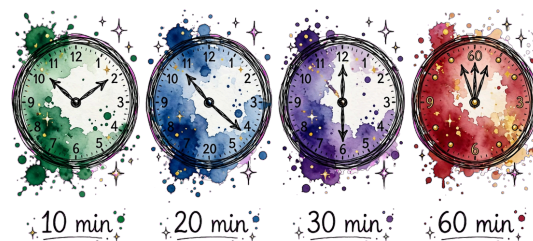
Tool 10, top to bottom. Never save sexual images of any child; links and usernames instead. Then block the offender's account. Do not delete your child's account or the messages.

Hour 3 to 12: the reports.

Platform report → Take It Down (if images exist or are threatened, even as a shield) → FPB hotline (SA) or CyberTipline → police FCS unit same day if there are threats, adult contact, images, money, or a meeting. Use the Chapter 11 report wording template. Get a case number.

Hour 12 to 24: the child again.

The reassurance script, repeated: *this does not define you, images can often be taken down, blackmailers rely on secrecy, and telling me was the right step.* Stay close. Keep it boring and warm. Crisis lines visible: 116 and 0800 567 567. I suggest booking professional support this week, not waiting to see if things get worse.



WEEKLY 10 MINUTE SAFETY REVIEW

Smaller than the monthly check. Sunday evening works. No settings, just presence.

- 1 Minute 1 to 3: sit where they are playing or scrolling. Watch. Ask nothing yet.

- 2 Minute 4 to 5: one genuine question about the content, not the safety: "what is this one about?"

- 3 Minute 6 to 7: one card from Tool 11, age appropriate, then drop it.

- 4 Minute 8: glance at your own week: did you post the kids anywhere public? Did you model phone down at meals?

- 5 Minute 9: anything from the warning signs list nagging at you? Note it; do not raid tonight.

- 6 Minute 10: end with something that is not about safety at all. The ritual is the door.

Date: _____