FAMILY NET CARE
DIGITAL PROTECTION AND EDUCATION



BOOKLET · 2026 EDITION

Digital Well-Being

A step-by-step guide for families and schools: from the first assessment to the screen agreement, from the risks to the help protocol.

FAMILYNETCARE.ORG

NOVEMBER 2026

How to use this booklet

This booklet takes a family or a school from the first assessment to agreed rules, step by step, in about 30 days. Each step ends in a concrete action and a ready-made template you can print or adapt.

WHO IT IS FOR

Parents and guardians, teachers, school teams and teenagers (age 13 and up, in the parts marked “For teens”).

ESTIMATED TIME

25 minutes to read; 4 weeks to put everything into practice (see the 30-day plan).

How to read it

1. Read Step 1 and complete the assessment before any conversation with your children.
2. Follow the steps in order; each one builds on the previous one.
3. Keep the “If something happens” and “Help channels” sections where you can reach them quickly (printed or bookmarked on your phone).
4. Use the ready-made templates as a starting point and adapt them to your home or school.

NOTICE

This booklet is educational material. It does not replace an assessment by a psychologist, pediatrician, lawyer or the authorities. In immediate danger in Brazil, call **190**. This edition keeps the Brazilian laws and help channels, because Family Net Care is based in Brazil; see “Help channels” for how to reach them from abroad.

Contents

00	Why this booklet exists · How design holds attention	Scenario, data and map
01	Family assessment	10 minutes
02	Agreeing on rules: the screen agreement	Ready-made template
03	Setting up devices, accounts and privacy	About 1 hour
04	Knowing the risks: signs and first steps	7 risks
05	Conversations by age group	Ages 6 to 18
06	If something happens: a 7-step protocol	Help channels
+	The law in plain language · For schools	Digital ECA, Penal Code, protocol
+	Templates · 30-day plan · Glossary · Sources	Closing

CONTEXT

Why this booklet exists

00

ILLUSTRATIVE SCENE

It is 11:40 p.m. and the glow of the phone still lights the bedroom ceiling. Nobody argued, nobody was careless: the app simply never tells you the night is over. For many families the problem is not a lack of care but a lack of method.

This booklet offers that method. The data below was checked against an official source or a recognized institution, and each item states the limits of what it allows us to conclude.

Ages 0–2: no screens · 2–5: up to 1 h · 6–10: 1–2 h · 11–18: 2–3 h per day

Brazilian Society of Pediatrics (SBP)

A recommendation from a medical body, not a law; use it as a reference for the family agreement. Disconnect at meals and 1 to 2 hours before bed.

100,077 reports in 2024, 33% fewer than the 150,847 in 2023

SaferNet, National Reporting Center

A report is not prevalence: it measures what reached the channel, not how many cases exist.

Digital ECA (Law 15,211/2025) in force since March 17, 2026

Federal Senate and Planalto

The law binds platforms; there is not yet a public study showing its effect on the risks.

Law 15,100/2025 restricts personal devices in basic-education schools, including at recess

Federal Senate

It has exceptions: teaching use, accessibility, health, necessity or danger.

WHAT THE EVIDENCE DOES AND DOES NOT LET US SAY

- Heavy screen use is associated with worse sleep, lower attention and more emotional distress in part of the studies; association does not prove that the screen is the cause.
- “Brain rot” is a popular expression, not a diagnosis. “Nomophobia” is also a descriptive term with no official diagnostic status.
- Gaming disorder is listed in the WHO’s ICD-11, but only a health professional can diagnose it.
- Screen-time statistics vary with method and sample, so this booklet does not mix them.

CONTEXT

How app design holds attention

Apps and games are designed to keep people using them. Understanding the techniques lifts the weight of guilt: difficulty stopping is not a character flaw of the child or the family. The map below organizes the topic into three questions.

1. Why it works

The mechanisms below are hypotheses backed by research, not certainties about any particular child.

- **Reward system:** novelty and small wins activate circuits tied to pleasure and motivation, which reinforces the habit of coming back.
- **Intermittent reinforcement:** when the prize is unpredictable (a rare item, a notification, a like), anticipation keeps the person trying again.
- **Fast gratification:** short content trains people to wait very little for a reward.
- **Self-control still developing:** the regions linked to planning and impulse control keep maturing into young adulthood, so children and teenagers have less defense against designs built to hook them.
- **Sleep:** screen use at night is associated with sleeping less and worse.

2. How it is done

TECHNIQUE	HOW IT WORKS	WHERE IT APPEARS	WHAT TO WATCH FOR AT HOME
Gamification	Points, badges, rankings and levels create endless goals	Games, study apps, social networks	“Just one more level”; irritation when stopping midway
Random rewards	Items drawn by chance, including paid ones (loot boxes)	Games	Requests to buy; charges on the card. Law 15,211/2025 (art. 20) bans loot boxes in games aimed at, or likely to be accessed by, children and teenagers
Push notifications	Alerts interrupt and pull the user back	Messengers, social networks, games	Checking the device with no alert; interrupted sleep
Infinite scroll and autoplay	There is no “end of page”; the next video starts by itself	Short videos, social networks	Losing track of time
Likes and social comparison	The number of reactions becomes a measure of worth	Social networks	Mood that swings with the response received
Recommendation algorithms	Show more of what has already held attention	All platforms	Narrower and narrower interests; repetitive content

TECHNIQUE	HOW IT WORKS	WHERE IT APPEARS	WHAT TO WATCH FOR AT HOME
Sound and color effects	“Victory” sounds and colors reinforce every action	Games, apps	High volume and brightness; difficulty switching off

3. What happens

Effects associated with excessive use.

Attention and learning

Difficulty focusing, remembering and sustaining long tasks.

Emotions and bonds

Anxiety without the device, social comparison, frustration and, in some cases, isolation and exposure to cyberbullying.

Behavior

Aimless scrolling, compulsive re-watching of videos and impulsive decisions.

LIMIT

Studies show associations, and the weight of each factor varies from person to person. If distress persists, the advice is to see a pediatrician or a mental health professional.

STEP 1

Family assessment

01

GOAL

Find out, in 10 minutes, where the home is protected and where it is not. Answer together as adults; this is not a test for the child and not a clinical diagnosis.

Check what already happens today

- [ ] The phone sleeps outside the child's or teenager's bedroom.
- [ ] Meals happen without screens, adults included.
- [ ] There is an agreed time rule, preferably in writing.
- [ ] Adults know which games and apps their children use and who they talk to in them.
- [ ] The children's profiles are private and location is turned off on social networks.
- [ ] Important accounts have a strong password and two-step verification.
- [ ] Adults know the minimum age stated in each app's terms of use.
- [ ] There has been at least one conversation about what to do if someone asks for an intimate photo or insults them online.
- [ ] The child knows they can report a problem without automatically losing the device as punishment.
- [ ] The family knows who to turn to in case of a crime or crisis (Step 6).

How to read the result

ITEMS CHECKED	READING	WHERE TO START
0 to 3	Little agreed protection	Steps 2 and 3 this week
4 to 7	Partial foundation	Complete the empty items and do Step 5
8 to 10	Solid foundation	Review the rules every 3 months

SIGNS THAT CALL FOR ATTENTION

A single occurrence proves nothing; the pattern and its duration are what matter.

- lies about or hides time spent on devices;
- strong irritation or anxiety without the device;
- sleep interrupted to use the phone;
- drop in school performance or loss of interest in activities once enjoyed;
- withdrawal from friends and family;
- unexplained spending on games or apps.

When several signs persist for weeks, the advice is to see a pediatrician or a psychologist.

STEP 2

Agreeing on rules: the screen agreement

02

GOAL

Turn loose limits into a clear agreement that applies to the whole household. A rule imposed without conversation does not last; a rule that is negotiated, written down and reviewed tends to be followed with less conflict.

Reference by age (SBP; adapt to each family and ask your pediatrician if in doubt)

AGE	REFERENCE TIME	WHAT TO AGREE ON
0 to 2 years	No screens	Play, cuddles, books; video calls with family can be arranged with the adults
2 to 5 years	30 min to 1 h a day, with an adult present	Content chosen by the adult; no screen to calm the child or at mealtime
6 to 10 years	Up to 1 to 2 h a day, always supervised	List of approved games and videos; device in a common area; no purchases
11 to 18 years	2 to 3 h a day, no “all-nighters”	Switch-off time; private profiles; a rule for photos and groups; phone out of the bedroom at night

SCREEN-FREE ZONES AND TIMES (FOR EVERYONE)

Meals · 1 to 2 hours before sleep · the bedroom at night · family conversations.

How to build the agreement, step by step

1. **Pick the moment.** A calm conversation, away from an argument and without a device in hand.

2. **Start with what matters to the child.** Ask what they like most about games and social networks; it shows interest and lowers their guard.
3. **Explain the reason.** “Sleeping well helps you learn and be in a good mood” works better than “because I said so.”
4. **Negotiate within firm limits.** Adults set what does not change (sleep, meals, safety); the child has a say in the rest (which hours, which games).
5. **Include the adults.** If parents use their phones at the table, the rule loses force. The agreement applies to everyone.
6. **Write it and sign it.** Use the Screen agreement tool on the website (ages 6 to 8, 9 to 10 and 11 to 12) or the template in this booklet.
7. **Set the consequences beforehand.** Choose proportionate, predictable consequences tied to the rule that was broken, and avoid taking the device away as the answer to every problem.
8. **Review in 30 days.** Rules change with age and maturity; adjust them together with the child.

SCREEN AGREEMENT · SHORT TEMPLATE TO ADAPT

Our family agrees that:

1. Devices stay off at meals and during the end-of-day conversation.
2. At night, devices sleep outside the bedroom, from ____ o’clock.
3. Weekdays: up to ____ of leisure screen time. Weekends: up to ____.
4. We do not install apps or make purchases without telling an adult.
5. We tell a trusted adult when something online makes us feel bad, knowing that telling is not a reason for punishment.
6. Adults follow the same table and bedtime rules.
7. We will review this agreement on ____ (date).

Signatures: _____ _____ _____

STEP 3

Setting up devices, accounts and privacy

03

GOAL

Reduce the risk surface with adjustments that take about an hour and last for months. Menu names change often; look for “Privacy,” “Security” and “Parental controls” in each app’s settings.

ITEM	WHAT TO DO	NOTE
Passwords	Use long, unique passphrases for every account; keep them in a password manager	Avoid birthdays, names and the same password across services
Two-step verification	Turn it on for email, social networks, games and app stores	An authenticator app resists attacks better than an SMS code; SMS is still better than nothing
Profiles	Make them private; review who follows; remove unknown contacts	A public profile makes it easier for strangers to make contact and to reuse photos
Messages and groups	Limit who can message or invite to groups	Check the groups the child has been added to
Location	Turn it off in photos, social networks and games	Photos showing a uniform, license plate or building front reveal routine
Parental controls	Use the system tools (for example, Google Family Link on Android and Screen Time on iPhone) and those of consoles and games	Helps limit hours, purchases and apps; it does not replace conversation
Purchases	Require an adult’s password or approval in the app store	Prevents impulse spending and “free skin” scams
Updates	Keep the system and apps up to date	Fixes security flaws
Open networks	Avoid opening important accounts on public Wi-Fi	Prefer mobile data
Minimum age	Check the terms of use before creating an account	The digital protection law also requires accounts up to age 16 to be linked to a guardian (see “The law in plain language”)

TRANSPARENCY

The child should know what is being set up and why. Hidden monitoring tends to break trust and encourages secret accounts.

FOR TEENS (AGE 13 AND UP)

Review your settings every three months; be wary of links with urgency (“your account will be banned”); never share codes you receive by message; if you lose access, tell a trusted adult immediately.

STEP 4

Knowing the risks: signs and first steps

04

GOAL

Recognize problems early, without panic. Each risk lists signs, first steps and the applicable rule (details in “The law in plain language”). In every case, the Step 6 protocol applies.

Cyberbullying

WHAT IT IS	Repeated intimidation through digital means: offensive messages, rumors, exclusion from groups, fake profiles, exposure of personal data.
SIGNS	Isolation, irritability, falling grades, changes in sleep and appetite, fear of or refusal to use the phone, sudden mood swings.
FIRST STEPS	Listen without minimizing; keep evidence; block and report on the platform; inform the school; seek psychological support if there is distress. Explain to the child that reporting is not “snitching.”

RULE Art. 146-A of the Penal Code (Law 14,811/2024): systematic intimidation and systematic virtual intimidation.

Online games, spending and excessive use

WHAT IT IS	Games use goals, rankings and random rewards to extend play time; some players lose control of their use.
SIGNS	Thinks about the game all the time, lies about time played, drops friends, sport and study, gets irritated when stopping, spends without permission.
FIRST STEPS	Play together once a week; agree on hours in Step 2; lock purchases; notice who the child talks to in the game; see a health professional when the game has harmed sleep, school or social life for weeks.
COMMON SCAM	Promises of a “free skin” or in-game currency that ask for a login, code or card. No legitimate game asks for your account password outside its own app.

Grooming

WHAT IT IS An adult approaches a child or teenager online to gain their trust and later exploit them sexually. The process is usually gradual: attention and flattery, a request for secrecy, distancing from other people, conversations that test limits and, finally, pressure or threats.

SIGNS An older online "friend" the family does not know; gifts or game credits; a conversation that moves to a private app; a request for secrecy; mood changes when reading messages.

FIRST STEPS Do not confront the adult; do not delete anything; keep the conversations; block only after saving the evidence; report (Step 6). The child is not at fault.

RULE Art. 241-D of the ECA: to groom, harass, instigate or coerce, through any means of communication, for a sexual purpose. Brazil's Superior Court of Justice (STJ) has held that "by any means of communication" refers to intermediary means, not to in-person conversation.

Intimate photos, sextortion and AI-made fake images

WHAT IT IS Requests for, exchange of or leaks of intimate images; blackmail to avoid disclosure (sextortion); composites that put a person's face on a nude body generated by software.

SIGNS Sudden fear of the phone, deleting accounts, requests for money or gift cards, a drop in mood.

FIRST STEPS Do not pay and do not send anything more; do not delete the messages; keep evidence of the request and the profile; report; offer support without blame.

NEVER FORWARD

An image of a child or teenager, not even "to show someone": producing, keeping or sharing this kind of content is a crime, and sharing increases the harm.

RULE Arts. 218-C and 216-B of the Penal Code; arts. 240 to 241-C of the ECA when the victim is under 18; art. 21 of the Marco Civil da Internet (removal on notice for non-consensual nudity).

Scams and fraud

SIGNS Urgency, an unexpected prize, a link received by message, a request for a code or password, a "support" profile.

FIRST STEPS Do not click; do not give out codes; change the password and turn on two-step verification; tell the bank if a card was involved; file a police report.

RULE Electronic fraud: art. 171, § 2-A, of the Penal Code.

Children’s photos and data (sharenting and AI)

WHAT IT IS Photos and information about children posted by relatives can be copied, combined with other data and used by third parties, including for composites.

FIRST STEPS Private profile; avoid uniforms, school, routine and location; do not post children in intimate situations (bath, changing clothes); ask relatives to take the same care.

RULE LGPD (Brazil’s data protection law), art. 14: the processing of children’s data must be in their best interest.

Repetitive viral content (“brain rot”)

WHAT IT IS Continuous consumption of short, repetitive videos. It is not a diagnosis; it is a popular name for a real concern about attention and sleep.

FIRST STEPS Time limits, content chosen together and offline alternatives the child enjoys.

STEP 5

Conversations by age group

05

GOAL

Keep the dialogue open. Children and teenagers who know they will be heard, and not punished right away, tend to speak up sooner when something goes wrong.

Five rules for any age

1. **Choose the moment.** Talking in the car, in the kitchen or on a walk works better than a formal "we need to talk."
2. **Start with open questions.** "What have you been enjoying watching?" opens more doors than "are you watching something wrong?"
3. **Listen to the end.** Interrupting to correct teaches hiding.
4. **Agree beforehand: telling does not bring automatic punishment.** Any consequence comes after understanding what happened. Taking the device away as an immediate response to a report teaches the opposite of what you want.
5. **Repeat, instead of giving one big lecture.** Short, frequent conversations build more trust than one long talk.

Guide by age group

AGE	FOCUS OF THE CONVERSATION	OPENING LINES	SUGGESTED AGREEMENTS
6 to 8 years	Simple rules, asking for help, not talking to strangers	"If something strange shows up on the screen, what can you do?" · "Who is that person talking to you in the game?"	Use only with an adult nearby; photos only with permission; "if something scares you, come and tell me"
9 to 12 years	Online friendships, secrets, game chats, cyberbullying, images	"Has anyone ever asked you to keep a secret on the internet?" · "What is the class group like?"	A known contact list; password kept with a guardian; no sending photos of face or body; hours from Step 2
13 to 15 years	Privacy, reputation, peer pressure, intimate photos, scams, online relationships	"What would you do if someone asked for a photo of you?" · "Do you know anyone who has been through this?"	Private profile; two-step verification; agree on what to do if an image leaks; tell someone before meeting a person known only online
16 to 18 years	Autonomy with responsibility, legal consequences, mental health, work and public image	"How do you decide who to trust online?" · "What do you think a future employer would see?"	Reviewing privacy settings together; the practice of reporting; knowing who to turn to; respect for other people's privacy

When your child does not want to talk

- Do not push on the first attempt; come back to the subject another day, in a light tone.
- Use outside situations: a news story, a series, a character's case.
- Show you are available: "If you ever want to tell me something hard, I will listen first and solve it together afterward."
- Persistent signs of distress (isolation, prolonged sadness, strong changes in sleep or appetite) justify seeking a health professional or the neighborhood health service.

FOR TEENS

If something strange happens online, it is not your fault. Scammers and ill-intentioned adults count on shame. Saving the messages, not replying, blocking afterward and telling someone you trust is always a good decision. There are free, confidential channels to ask for help (see Step 6).

STEP 6

If something happens: a 7-step protocol

06

GOAL

Act calmly and in the right order. The rush to delete, confront or punish usually destroys evidence and pushes the child away.

1. **Welcome the child.** Say, in few words: “You did well to tell me. It is not your fault. We will sort this out together.” Avoid questions that sound like accusations (“why did you send it?”).
2. **Do not delete and do not confront.** Do not remove conversations, profiles or groups, and do not answer the aggressor or the blackmailer. This preserves evidence and avoids retaliation.
3. **Keep evidence without redistributing illegal content.** Take screenshots showing the profile name, date, time and the address (link) of the conversation; note usernames and numbers. When it involves an intimate image of a child or teenager, **do not forward the file to anyone**, not even relatives or friends: document only what is necessary (for example, the profile, the link and the message) and hand the rest directly to the authorities.
4. **Block and report on the platform.** After saving the evidence, block the profile and use the app’s reporting tool. The platform may remove the content, but that does not replace reporting to the authorities.
5. **Report to the authorities.** Choose the channel by case (table below): Disque 100, SaferNet, the police station (including an online police report, where available in the state), the Conselho Tutelar.
6. **Tell the school**, if it involves classmates or the school environment, so that it can apply its protocol (section “For schools”).
7. **Look after emotional health.** Watch sleep, mood and appetite over the following weeks; see a psychologist or health unit if there is distress. In immediate risk in Brazil, call 188 (CVV) or 190.

Help channels (Brazil)

SITUATION	CHANNEL	NOTES
Violation of the rights of children and teenagers (abuse, exploitation, grooming)	**Disque 100** (Human Rights Hotline)	Free, 24 hours, accepts anonymous reports. From outside Brazil, use WhatsApp +55 61 99611-0100 or Telegram *DireitosHumanosBrasil*
Crimes and violations on the internet	**SaferNet Brasil** new.safernet.org.br/denuncie	Receives reports of illegal online content and forwards them to the authorities; works through the website, so it can be used from anywhere
Psychological guidance and support for people affected by online situations	**Canal Ajuda (SaferNet)** canaldeajuda.org.br	Guidance service; does not replace a psychologist
Emotional distress, thoughts of self-harm	**CVV 188**	Free, 24 hours, within Brazil; also by chat and email on the CVV website
Emergency, immediate threat	**190** (Military Police)	For present danger, within Brazil
Formal report of a crime	**Police station** (*delegacia*, preferably one specialized in cybercrime or child protection, where available)	Bring screenshots, links and profile data
Children's rights in your city	**Conselho Tutelar** (Guardianship Council)	Serves families and schools; applies protection measures
Irregular processing of children's and teenagers' data (Digital ECA)	**ANPD** gov.br/anpd	The national authority's channel for petitions and reports

CALLING FROM OUTSIDE BRAZIL

The short numbers (100, 188, 190) work only inside Brazil. From abroad, use the websites above and the WhatsApp or Telegram channel of Disque 100. Family Net Care can also be reached through the contact form at familynetcare.org (Contact page).

WHAT TO TELL THE CHILD AT THE END

Explain what will be done, who will be told and that they will not be blamed. Agree on a simple signal (a word or a note) to ask for help in the future without having to explain everything on the spot.

REFERENCE

The law in plain language

GOAL

Give a quick reference to what Brazilian law provides. This table is informational and does not replace legal advice. Penalty values are not reproduced because several provisions were recently amended: always check the current text at planalto.gov.br.

Conduct × rule

SITUATION	REFERENCE RULE	IN PLAIN WORDS
Insults, name-calling, false accusations	Penal Code, arts. 138 (calumny), 139 (defamation), 140 (insult)	Crimes against honor, which also exist in the digital environment
Threats	Penal Code, art. 147	Promising unjust and serious harm to someone
Systematic intimidation (bullying and cyberbullying)	Penal Code, art. 146-A (Law 14,811/2024)	Intimidating repeatedly, including over the internet
Sharing nudity or an intimate scene without consent; composites and fake nude images	Penal Code, arts. 218-C and 216-B, sole paragraph	Sharing or creating this kind of content can be a crime. How this applies to AI-generated images is still being settled in the courts
Images of nudity or sex involving anyone under 18	ECA, arts. 240, 241, 241-A, 241-B and 241-C	Producing, selling, sharing, keeping or simulating this material is a crime, even if the image was sent by the teenager themselves
Grooming of a child or teenager	ECA, art. 241-D	Approaching through a means of communication for a sexual purpose
Breaking into an account or device	Penal Code, art. 154-A	Improper access to someone else's device or account
Pretending to be someone else to gain an advantage or cause harm	Penal Code, art. 307 (false identity)	Using a name or identity that is not yours
Scams, electronic fraud	Penal Code, art. 171, § 2-A	Deceiving by electronic means to gain an advantage
Inducing or instigating self-harm or suicide	Penal Code, art. 122 (wording of Law 13,968/2019)	Instigating, inducing or assisting is a crime
Copying and sharing someone else's work without permission	Law 9,610/1998 (copyright)	Texts, images and videos have an author

SITUATION	REFERENCE RULE	IN PLAIN WORDS
Use of a person's image	Civil Code, art. 20	Publishing a person's image may require authorization
Children's personal data	LGPD (Law 13,709/2018), art. 14	Processing must serve the child's best interest
Harm to another person	Civil Code, arts. 186, 927 and 932, I	Whoever causes harm must repair it; parents may be held civilly liable for minor children under their authority

Digital ECA (Law 15,211/2025)

The law regulates digital services accessible to children and teenagers. Key points, with the article reference:

- **Best interest and full protection** as principles for digital products and services (art. 7).
- **Duties of providers** to prevent risks and adopt age-appropriate measures (arts. 17 and 18).
- **Loot boxes** in electronic games: prohibited for this audience (art. 20).
- **User accounts up to age 16** must be linked to a legal guardian (art. 24).
- **Removal of content** involving child sexual exploitation or abuse and other violating content without a court order, on notice (art. 29).
- **Administrative sanctions** applied by the ANPD, with fines of up to 10% of revenue in Brazil, capped at R$ 50 million per infraction (art. 35).
- **Decree 12,880/2026** regulates age verification (art. 24, with eleven items) and the role of app stores (art. 25).

SCHOOL AND PHONES

Law 15,100/2025 governs the use of portable electronic devices in basic-education schools, regulated by **Decree 12,385/2025**. It does not set a minimum age for social networks.

IMPORTANT NOTES

- Teenagers aged 12 to 17 answer for an **infraction** (*ato infracional*) under the ECA, not for an ordinary prison sentence; civil liability for damages may fall on their guardians.
- Children up to age 11 who commit an act similar to a crime receive protection measures, not socio-educational measures.
- Each family's situation needs a case-by-case analysis by a lawyer or the Public Defender's Office (Defensoria Pública).

INSTITUTIONS

For schools

GOAL

Support teaching teams in organizing a screen-use policy, a protocol for incidents and educators' digital conduct, in line with Law 15,100/2025.

1. Institutional phone policy

Law 15,100/2025 restricts students' use of portable electronic devices during classes, recess and breaks, with exceptions for teaching purposes, accessibility, health and situations set out in the rule. To put the rule into practice:

- **School rules:** record the rule, the exceptions and the consequences clearly for students and families.
- **Storing devices:** define where and how devices are kept (switched off in the backpack, a locker, a box per class) and who is responsible for them.
- **Awareness activities:** include the topic in projects, discussion circles and parent meetings.
- **Welcoming spaces:** offer a listening ear (educational counseling, a school psychologist where available) to students in distress.
- **Staff training:** train teachers and staff to recognize signs and trigger the protocol.

2. Institutional checklist

- [ ] School rules updated with the phone policy and exceptions
- [ ] Formal communication to families (meeting and document)
- [ ] Written digital-incident protocol known to the staff
- [ ] A reference person (and a substitute) to receive reports
- [ ] Updated contacts: Conselho Tutelar, police station, Disque 100, local health service
- [ ] A safe reporting channel for students, including anonymous
- [ ] An annual digital education activity for each class
- [ ] Policy review at least once a year

3. Digital incident protocol

1. **Recording:** whoever receives the report notes the date, the people involved, what was said and where it happened, without interrogating or exposing the victim.
2. **Initial assessment:** management and counseling assess seriousness and immediate risk. Is there a risk to physical or emotional integrity? Is a crime suspected?

3. **Preserving evidence:** keep screenshots and links; **do not** copy, circulate or store intimate images of minors on school devices or in groups; hand them to the authorities when requested.
4. **Decision:** apply the educational and disciplinary measures set out in the school rules, proportionate and with the right of those involved to be heard.
5. **Communication:** inform the families of the parties involved; when a crime or rights violation is suspected, contact the **Conselho Tutelar** and the **police** as the case requires.
6. **Follow-up:** revisit the situation with the victim and the person who caused the harm after a few weeks, recording developments.

4. Educators' digital conduct

- Keep **professional profiles separate** from personal ones.
- Use only **official channels** (the school platform, institutional email) to talk to students; avoid private conversations on personal apps.
- In family groups, **do not expose** students' names, grades, photos or incidents.
- Do not publish images of students without families' authorization and a clear teaching purpose.
- When a student confides in you, do not promise absolute secrecy: explain that some cases require involving other people to protect them.

TOOLS

Ready-made templates

Template 1 · “Before you post” checklist

For families, students and educators. If any answer is “no” or “I don’t know,” it is worth waiting.

- [ ] Is the image or information mine, or do I have permission from the people in it?
- [ ] Does it show a uniform, school, address, license plate, routine or location?
- [ ] Could anyone feel exposed, humiliated or embarrassed?
- [ ] Would I be comfortable if a stranger, a future employer or a distant relative saw it?
- [ ] Is my profile private and has my follower list been reviewed?
- [ ] Is it a child in an intimate situation (bath, changing clothes, illness)? If so, do not post.
- [ ] Is the information true? Did I check the source before passing it on?
- [ ] Could the content be copied and used for a scam or a composite?
- [ ] Would I post this five years from now without regret?
- [ ] If the post causes a problem, do I know how to remove it and who to ask for help?

Template 2 · Image use authorization form

NOTICE

A template to adapt. Before institutional use, have it reviewed by legal counsel. For anyone under 18, authorization is given by the legal guardian.

IMAGE USE AUTHORIZATION FORM

I, _____, CPF (Brazilian taxpayer ID) no. _____, legal guardian of _____, authorize _____ (institution/project) to use images (photographs and videos) of the minor identified above, exclusively for:

- ☐ Internal educational materials
- ☐ Institutional website
- ☐ The institution's social networks
- ☐ Other: _____

Conditions

1. The image will not be used for commercial purposes or linked to information that would allow the child to be located (address, routine, full name, identifiable school uniform), unless expressly authorized.
2. Use will last _____ months from the date of signature.
3. The authorization may be revoked at any time, in writing, without prejudice to the student; the institution will remove the images from the channels under its control within _____ days.
4. Personal data will be processed in accordance with the LGPD, in the child's best interest.

Place and date: _____ Guardian's signature: _____

Template 3 · Parent meeting agenda (60 minutes)

TIME	ACTIVITY	NOTES
0–10 min	Welcome and goal of the meeting	Present the school's policy on phones and screens
10–25 min	Scenario and risks	Use Step 4 of this booklet, in plain language, without panic and without exposing real cases
25–40 min	Group activity	Each group creates a "family agreement" with Step 2 and presents one rule
40–50 min	How to talk and what to do if something happens	Steps 5 and 6; present the help channels
50–60 min	Questions and agreements	Hand out the booklet and record families' suggestions

PUTTING IT INTO PRACTICE

30-day plan

GOAL

Turn the booklet into routine, one stage per week. Adjust to the pace of the family or school.

WEEK	FOCUS	ACTIONS	EXPECTED RESULT
1 · Assessment	Steps 1 and 2	Complete the assessment; list the apps and games in use; record screen time for three days without demanding changes	A real picture of use, without judgment
2 · Agreements	Steps 2 and 3	Build the family (or class) agreement; set up privacy, passwords, two-step verification and device controls; define screen-free zones and times	A written agreement, visibly posted
3 · Conversation	Steps 4 and 5	Talk about the risks by age group; use a hypothetical situation; agree on the signal for asking for help	The child knows what to do and who to tell
4 · Protocol and review	Step 6	Save the help channels on guardians' phones; rehearse the 7 steps; review the agreement and adjust what did not work	Family or school prepared and agreement reviewed

After the 30 days

- Repeat the assessment every three months.
- Review the agreement whenever there is a change of age, school, device or social network.
- Follow legal and platform news in the Family Net Care website articles.

Glossary

Age verification: a digital service checking the user's age by means set out in regulation.

Grooming: an adult's approach to a child or teenager, online or through another means of communication, for a sexual purpose.

Recommendation algorithm: a system that decides what appears next in the feed or videos, based on the user's behavior.

Brain rot: a popular name for continuous consumption of repetitive, low-value digital content; not a medical diagnosis.

Parental controls: tools to set limits, filters and supervision of device and app use.

Cyberbullying: repeated intimidation through digital means.

Deepfake: a fake image, audio or video created or altered by artificial intelligence to look real.

Digital ECA: Law 15,211/2025, which sets duties for digital services aimed at children and teenagers.

LGPD: Brazil's General Personal Data Protection Law (Law 13,709/2018).

Loot box: a game item whose content is drawn by chance, usually obtained with real money.

Phishing: a scam that uses fake messages or pages to obtain passwords, codes or data.

Sextortion: blackmail threatening to share intimate images, usually to obtain money or more images.

Sharenting: the habitual posting, by parents or guardians, of photos and information about their children.

Two-step verification: an extra layer of security that requires, besides the password, a second code or confirmation.

CLOSING

Sources, website articles and originality note

Family Net Care website articles by chapter

BOOKLET CHAPTER	RELATED ARTICLES (WEBSITE ID)
Steps 1 and 2 · Assessment and screen agreement	1 (parental control vs. parental mediation), 14 (the right age for social networks and games), 16 (algorithms and phone addiction), 15 (parental phubbing)
Step 3 · Settings and protection	1, 17 (who your children talk to), 18 (chatbots)
Step 4 · Cyberbullying	4 (excessive use and cyberbullying), 6 (cyberbullying and suicide risk)
Step 4 · Games, spending and addictive design	2 (how games engage), 10 (game addiction), 11 (games designed to hook), 20 (free skins and scams)
Step 4 · Grooming	9 (digital predators), 17
Step 4 · Images, AI and data	5 (protecting images in the AI era), 12 and 13 (photos and AI), 19 (sharenting)

BOOKLET CHAPTER	RELATED ARTICLES (WEBSITE ID)
Step 4 · Viral content	3 (brain rot and short videos)
Mental health and excessive use	3, 6, 15, 16, 18
Law and public policy	8 (NR-1 and phone use at work), legal articles published on the website
Nomophobia	7 (nomophobia and productivity), 8

Sources consulted

Legislation (official texts at planalto.gov.br): Penal Code (Decree-Law 2,848/1940), arts. 122, 138 to 140, 146-A, 147, 154-A, 171 § 2-A, 216-B, 218-C, 307; Child and Adolescent Statute (Law 8,069/1990), arts. 240 to 241-D; Law 15,211/2025 (Digital ECA) and Decree 12,880/2026; Law 15,100/2025 and Decree 12,385/2025; Law 14,811/2024; Law 13,709/2018 (LGPD), art. 14; Law 12,965/2014 (Marco Civil), art. 21; Law 9,610/1998; Civil Code, arts. 20, 186, 927 and 932.

Channels and guidance: Ministry of Human Rights and Citizenship (Disque 100); SaferNet Brasil and Canal Ajuda; Centro de Valorização da Vida (CVV); ANPD; Federal Senate; Brazilian Society of Pediatrics (guidance on screen use).

Own content: the “Vicious Design” mind map and articles published on the Family Net Care website.

PLEASE NOTE

Penalty values and the application of the rules to AI-generated images are not detailed in this booklet because they are subject to change and to case-law consolidation. Always check the current text.

ORIGINALITY NOTE

The text of this booklet was written from scratch by the Family Net Care team. Third-party materials served only as an inventory of topics; no passage was copied. The templates (agreement, checklist, form, agenda, 30-day plan) are original. The numbers and rules cited were checked against official sources; where there was no confirmation, the data point was left out.

November 2026 edition



Protecting means talking, agreeing and acting together.

Free articles, tools and materials for families and schools.

familynetcare.org

Educational material. It does not replace an assessment by a psychologist, pediatrician, lawyer or the authorities. In immediate danger in Brazil, call 190.