

Keeping your teenager safer online.

A do-it-this-weekend companion to the *Regulating the Teen Internet* series — ordered by what genuinely reduces harm, not what merely feels reassuring. Work down it, and keep the last page where you can find it in a hurry.

THE ONE RULE — BUILD THIS FIRST

Your child must believe, correctly, that telling you about something bad online will not cost them the device.

Ofcom found that around three-quarters of 11–17s saw harmful content in a single four-week window — and only about fifteen per cent told an adult. The commonest reason for silence is the fear that reporting a frightening message gets the phone taken away. If you fix one thing, fix that. A script worth memorising, from UNICEF: *"I'm glad you told me. You are not to blame, and I'm here to help. Let's figure it out together."*

THE REORDERING MOST HOUSEHOLDS GET BACKWARDS

The largest evidence we have — Chen & Shi's meta-analysis of fifty-two studies — found that **restriction and blocking cut screen-time hours, but conversation, co-use and teaching are what cut exposure to harm**. Different levers. Most families pull hard on the first and barely touch the second. The conversation is the primary control; everything technical below is a supporting layer that stops casual, accidental exposure — real value, but not the main event.

| The posture, in five layers

1	The conversation LOAD-BEARING WALL	Talk early, talk often. Curious, low-stakes, frequent — not one solemn Big Talk. Catches everything the technical layers miss. The one layer that does not leak.
2	The device LOCKS ON THE DOORS	Screen Time / Family Link / Microsoft Family Safety. Travels with the child into every app and network. Only as strong as the password behind it.
3	The platforms WINDOWS A STRANGER CLIMBS THROUGH	Audited by function, not brand: lock <i>who can contact the child</i> down to people they know. Settings change constantly — re-check.
4	The network FENCE AT THE END OF THE GARDEN	Broadband filter + a DNS filter for the whole house. Cheap, ten minutes. Bypassed by a VPN or mobile data — coarse net only.
5	The reporting routes EMERGENCY SERVICES	The numbers and sites you hope never to use. Bookmark them while it is calm. See the last page.

No single layer holds on its own. A determined threat has to get through all five — and a child who will actually *tell* you when something is wrong sits underneath the lot.

| Layer 2 — the device

The device is the only place that is always, unavoidably, in the room with the child. Set protections here and they hold on mobile data, on a friend's Wi-Fi, and inside apps — because it all runs on that device.

PLATFORM	WHERE TO GO, AND WHAT TO TURN ON
iPhone / iPad SCREEN TIME	Set up a Child Account in Family Sharing, then Screen Time : Downtime, App Limits, Content & Privacy Restrictions (web filtering, age-rated app/media limits, block installs & deletions), and — switch it on — Communication Safety , which detects and blurs nude images in Messages and FaceTime on the device itself.
Android / Chromebook FAMILY LINK	Google Family Link : app approval, screen-time and bedtime schedules, content-maturity limits, and SafeSearch locked on .
Windows / Xbox FAMILY SAFETY	Microsoft Family Safety : activity, screen-time and content limits across PC and console.

THREE HONEST CAUTIONS

- 1 • The lock is only as strong as its password.** On Apple, the Screen Time passcode can be reset by anyone who knows the *Apple Account* password used to set it up — so that must be a password your child does not have. This is the commonest way these controls quietly fail: not defeated, just unlocked.
- 2 • It is a seatbelt, not a force field.** Roughly two in five UK children report getting around age checks and controls of one kind or another. A determined teenager with a second-hand phone you never configured will defeat most of this. Raise the floor anyway — it stops most casual and accidental exposure — but do not mistake a configured device for a solved problem.
- 3 • The highest-value setting isn't in a menu.** It is a rule: **the phone charges overnight outside the bedroom**. It is the one control with no bypass — a phone on the kitchen counter cannot be doomscrolled at 2am or used to send a message a child will regret. A £3 charging habit outperforms most of the software.

| Layer 4 — the network

The weakest layer, but nearly free and worth ten minutes as a whole-home floor.

- Every UK broadband provider — **BT, Sky, TalkTalk, Virgin** — offers account-level filtering you can switch on to block adult categories across the whole house.
- For more control, point your router's DNS at a filter: **Cloudflare for Families (1.1.1.3)** or **NextDNS** blocks whole categories of site for every device on your Wi-Fi.

BE CLEAR-EYED ABOUT WHAT THIS DOES NOT DO

It blocks whole domains — so it cannot filter one bad video on a site you otherwise allow, and it cannot see inside apps at all. It is trivially bypassed by a VPN, by switching from Wi-Fi to mobile data, or by changing the phone's DNS. Treat it as a coarse net that catches accidental stumbles for the household — useful and cheap, and not to be trusted an inch further.

Layer 3 — audit the platforms by function

The harm follows a *function* — stranger contact with your child — not a brand. Run this four-question audit across every app and game they use, together, one evening, devices on the table. It works better as archaeology done *with* them than as a raid.

☐	Can strangers contact them here? Not "is it a social network" — can an unknown account send a message, friend request or party invite?
☐	Is there a private channel? DMs, whispers, party chat, voice — the places moderation cannot easily see.
☐	What do the settings currently say? Nearly every platform defaults more open than you would choose. Close them.
☐	Where would the conversation move to? "Let's talk on [somewhere else]" is the single most important tripwire a child can learn to notice and tell you about.

Settings genuinely worth your evening

Platforms change these constantly — treat the specifics as a starting point and check the current app.

PLATFORM	WHAT TO SET
Roblox A SOCIAL PLATFORM IN A GAME'S CLOTHING	Link your own (age-verified) account to enable Parental Controls : set a content-maturity ceiling , set an Account PIN so the child can't reverse your settings, and configure communication by age . Since Jan 2026 chat sits behind a facial age check — but that governs Roblox's <i>own</i> chat, not chat built inside individual games. The PIN and maturity ceiling are your real levers.
Discord	Turn on Family Centre (shows who your teen friends and messages, not the content), set who can DM to friends-only, keep sensitive-content filters on. Age-assurance changes now default teens to stricter settings.
Snapchat	Confirm Ghost Mode is on so location isn't shared (it's the default — check it by hand), set Contact Me to friends-only, and link Family Centre .
Instagram & TikTok	Both run Teen Accounts defaulting under-16s to private, restricted messaging and content filters. Set up supervision (Meta Family Centre ; TikTok Family Pairing) so loosening them routes to you. On TikTok, under-16s can't send or receive DMs at all.
YouTube	Younger children: the separate YouTube Kids app with search turned off. Older: a supervised account via Family Link with a content level set. Restricted Mode on the main app is per-device and easily switched off — don't lean on it.

The pattern under all of them is the same: lock *who can contact the child* down to people they actually know, and put a PIN or linked-parent approval between the child and the ability to undo it. You are not surveilling the conversation — you are making sure a stranger can't start one.

| Two threats worth knowing by name

Grooming — patient, and rarely the stranger-danger cartoon

An adult, often posing as younger, offers attention, flattery, advice and small gifts, builds a bond over weeks, then steers the conversation *off* the original platform onto something private: "let's talk on [somewhere else]." That platform-switch is the tripwire to teach. NSPCC warning signs: new secrecy about time online, an older boyfriend or girlfriend, unexplained gifts or money, going missing, withdrawal, or sexual language beyond their years. None is proof; together they are a reason to gently open the conversation.

Sextortion — fast, financially motivated, aimed at teenage boys

An attractive stranger makes contact, moves quickly to sexual chat, persuades the young person to send a nude — then instantly threatens to send it to family and friends unless they pay. Demands escalate within the hour. The NCA found three-quarters of boys didn't recognise a nude-image request as a warning sign. **Talk to your sons about this specifically, before it happens** — the shame is engineered to keep them silent.

IF IT HAPPENS — DO

- + Reassure them it is **not their fault** — they were deliberately deceived, and telling you was right.
- + **Keep the evidence** — messages, the offender's profile, links to anywhere images were shared.
- + Deactivate the account rather than delete it.
- + Stop all contact and **block** on every platform.
- + Report it (below). If the child is in immediate danger, call **999**.

DO NOT

- × **Do not pay.** It doesn't stop it — it marks the victim as exploitable and brings more demands.
- × **Do not delete everything.** Police need the evidence.
- × Do not confront the offender directly.
- × Do not let them handle it alone in silence.

| When it goes wrong — the routes that work

The names matter; parents' guides muddle them constantly. Report to the platform *as well*, keep the reference number, and preserve evidence *before* you block.

A child is in immediate danger	999 — everything else waits
Grooming, or an adult contacting a child sexually online	CEOP Safety Centre · ceop.police.uk/Safety-Centre (the NCA reporting route — not "CEOP Education", which is advice only)
A nude image of an under-18 that needs taking down	Report Remove — Childline & IWF, free (adults 18+: StopNCII)
Child sexual abuse imagery you've encountered	Internet Watch Foundation · iwf.org.uk (report anonymously)
Harmful-but-legal content, or a platform ignoring your report	Report Harmful Content · reportharmfulcontent.com
The child needs someone to talk to	Childline · 0800 1111 free & confidential
You, the adult, need advice about a child you're worried about	NSPCC Helpline · 0808 800 5000 even if unsure it's serious
Non-emergency police	101
A family dealing with the aftermath of tech-assisted abuse	Marie Collins Foundation

The bottom line: governments regulate platforms; parents raise people. The law arriving next spring will leak. The protections that hold are the ones in your house — the device you configured, the settings you closed, and a child who knows they can come to you first and will not lose the phone for telling the truth.