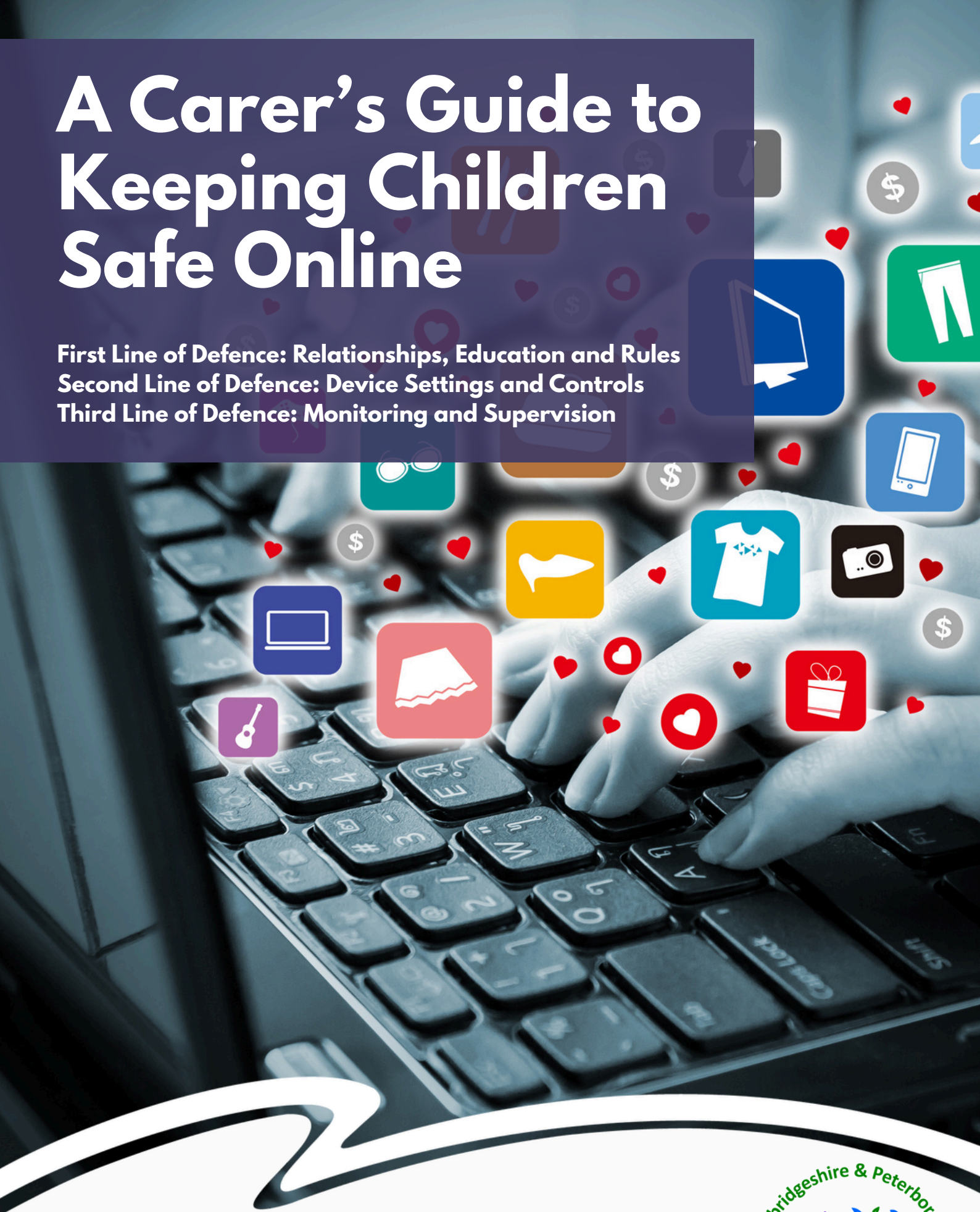
A Carer's Guide to Keeping Children Safe Online

First Line of Defence: Relationships, Education and Rules
Second Line of Defence: Device Settings and Controls
Third Line of Defence: Monitoring and Supervision



Cambridgeshire Constabulary

NHS Central East Integrated Care Board

Peterborough City Council

Cambridgeshire & Peterborough Safeguarding Adults & Children Partnership Boards

A Carer's Guide to Supporting Safe Online Behaviour in Children

It is important to recognise that children can be very skilled at hiding their online activity or finding ways around safety settings. Even children who are generally well-behaved can find themselves exposed to, or engaging with, inappropriate or harmful content online. This can often happen unintentionally, and every parent or carer should consider this possibility.

When children view material that is sexual in nature, it can trigger curiosity or a desire to seek it out again. Regardless of a child's upbringing, values or beliefs, such content can feel exciting or stimulating. This can lead to children becoming drawn to revisit such material, and they may find creative ways to access it repeatedly.

As a parent or carer, you are responsible for the safety of the children in your care, and that includes how they use devices and engage with the online world. Taking steps to safeguard children's developing minds helps to protect them from harmful content, exploitation, and exposure to material that could place them at risk of harm or getting into trouble.

It is important to develop a strong set of strategies to help keep children safe online. This should begin with open conversations and setting clear rules and boundaries, supported by the use of device settings, parental controls and monitoring tools where needed. We recommend having a shared agreement in place. These should be clear, age-appropriate, agreed by everyone involved, and regularly reviewed as children grow and their needs change.

This guide outlines three key lines of defence to help safeguard children. The first line of defence focuses on everyday digital parenting. The second line of defence covers the use of built-in device settings, while the third line of defence involves active supervision and monitoring.

Carers are encouraged to draw from each area to build a balanced and flexible approach that suits the age, needs and circumstances of each child.

It is important to think about all devices that can access the internet, including mobile phones, tablets, laptops and gaming consoles.

See the glossary at the end of this document to better understand relevant key and technical terms.

National Stats

70% of children aged 9–13 say they have been exposed to harmful content or experiences online*

27% of children reported seeing pornography online by age 11. Some said they were as young as **6** at first exposure**

59% of children and young people said they had seen pornography **by accident**, often through social media platforms**

**Internet Matters (2024) & **Children's Commissioner for England (2025)*

First Line of Defence: Relationships, Education and Rules

Open Communication and Education

Talk regularly about online safety, privacy, and respectful behaviour.
Discuss risks like cyberbullying, grooming, and inappropriate content.
Encourage questions and create a non-judgemental space for conversations.

Set Rules and Boundaries Together

Create a **family agreement** or a **digital use contract.**
Agree on screen time limits, appropriate apps, and online conduct.
Encourage device-free zones (e.g., bedrooms at night, mealtimes, school, etc.).

Adults to Model Healthy Digital Behaviour

Demonstrate balanced use of technology.
Show children how to spot trustworthy sources and to think critically about what they see online.

Feel free to discuss these options with professionals for extra support.

Second Line of Defence: Device Settings and Controls

Review App Permissions and Privacy Settings

Check what data apps collect & **limit permissions** (e.g., camera, mic, contacts).
Enable **screen time reports** to monitor usage patterns.
Disable location sharing unless necessary.
Turn on **safe search filters** in browsers and YouTube.
Ensure social media accounts (if applicable) are **private** & friend lists are known.

Lock Down the Device

Use 'kiosk mode' or 'child profiles' to **limit access** to approved apps.
Disable app stores or require **parental approval** for every action.
Use **remote lock** or **wipe features** in case of loss or misuse.



Third Line of Defence: Monitoring and Supervision

Soft Monitoring (with digital tools)

Use tools like Google Family Link, Apple Screen Time, or Microsoft Family Safety to:
Monitor app usage
Set time limits
Approve app downloads

Active Monitoring (with digital tools)

Use parenting apps (with transparency) to:
View browsing history and social media activity
Filter or block inappropriate content
Customise filters by age and maturity
Block specific websites or categories
Restrict app downloads to age-appropriate content

Manual Device Checks

In certain situations, especially with younger children or where there are safeguarding concerns, it may be appropriate to check a child's device directly.
This might include reviewing of messages, photos, browsing history, or recent downloads
Looking for signs of risky behaviour or exposure to harmful content
Always do this openly and with the child's knowledge, as part of a wider safeguarding approach.
Frame checks as a protective measure, not a punishment.
This should be included in any digital agreement.



Details on safety settings and monitoring apps

Getting Started with Device Safety Settings (2nd line of defence)

We recognise that not all carers feel confident navigating digital devices and online safety settings. If this applies to you, we encourage self-directed online learning to help you follow the steps outlined in the second line of defence.

Devices such as laptops, phones, tablets and games consoles *(for example, Nintendo Switch, Xbox and PlayStation)* can all be used to go online, including browsing the internet, watching content and messaging others.

Most of these devices have built-in parental controls, and many can also be linked to parental control apps, although features may vary depending on the device.

We have not included detailed instructions in this guide, as device systems change frequently. However, finding reliable guidance can be straightforward if you follow these steps:

1. Identify the device your child will be using.
Is it an Apple device *(e.g. iPhone, iPad)* or an Android device *(e.g. Samsung Galaxy A14, Motorola G73)*?

2. Search for guidance on the internet using clear, specific terms.
Try typing into a search engine:

- "How to limit app permissions on [device name and model]"
- "How to enable screen time reports on [device name and model]"
- "How to turn on safe search filters in [browser name] on [device name]"

These searches will usually lead to written guides or video tutorials *(e.g. YouTube)* that walk you through the steps visually. Many carers find video guides especially helpful.

Make sure all devices are updated with the latest software.



Finding Monitoring Apps (3rd Line of Defence)

The third line of defence involves using monitoring tools and apps to supervise device use. These tools can support carers in maintaining oversight in a way that is transparent, proportionate, and tailored to the child's age and needs. We recommend using well-supported monitoring tools so you can access the latest features, functionality and security updates.

Monitoring apps vary in features, cost and compatibility, so we recommend conducting your own research to identify options that suit your needs. You might begin by searching:

- "Best parental control apps for Android/iPhone"
- "Compare Qustodio vs Bark vs Net Nanny"
- "Free parental monitoring apps"

Look for reviews, comparison charts and video walkthroughs to help you decide. Many apps offer free versions with basic features such as screen time limits, content filtering and app approvals. Availability, features and user experience may change over time, and no single app provides complete protection.

Our own search (Oct 2025; reviewed June 2026) identified the following widely used tools, which you may wish to explore as a starting point:

Qustodio: (Offers strong web filtering, screen time limits, and detailed activity reports; Works across Android, iOS, Windows, Mac, and Chromebook)

Net Nanny: (Real-time content filtering and profanity masking; Includes app blocking, screen time management, and alerts)

Bark: (Monitors texts, emails, and 30+ social media platforms; Uses AI to detect risks like bullying, grooming, or explicit content)

Norton Family: (Ideal for families with multiple children; Offers search term tracking, time limits, and location monitoring)

Kaspersky Safe Kids: (Includes content filtering, app usage tracking, and battery monitoring; Good entry-level option for younger children)



Discussion points with children

Plan some discussion points to help children understand and feel included in the steps you take to keep them safe online. These conversations are an important part of building trust and transparency. Below are some ideas and prompts you can use. Feel free to adapt the language and approach to suit each child's age, maturity, and individual needs.

"Let's talk about how to stay safe online, just like we talk about crossing the road safely. If something online makes you feel weird, confused, or upset, you can always tell a grown-up you trust."

"We can agree on when and how to use your phone or tablet. That might mean no phones at bedtime or only using certain apps. These rules help keep things fun and safe."

"We can turn on special settings and use apps that help block rude or scary stuff. It's like putting up safety signs or a shield on your device."

"There are apps that help me/us see how much time you spend online and what you're doing. It's not spying; it's just checking in to help you stay safe."

"We can set up your device to only show a few apps that are just right for you. It's like having your own special playground online."

"Sometimes, we/I might need to check your phone or tablet to make sure everything is safe. This could mean looking at messages, photos, or websites you've visited. It's not because you're in trouble. It's because we care about you and want to help if anything goes wrong. We might also block apps or websites that aren't right for your age, so you only see things that are fun and safe."



Apps and Platforms carers should be aware of

This is not an exhaustive list. New apps are released regularly, and existing ones can change quickly. It's important to stay informed by checking your child's app usage and keeping up with online safety guidance (Reviewed June 2026).

Popular Apps / Online Platforms & Potential Safety		
TikTok	• Algorithm can expose children to sexualised, violent, or harmful content quickly. • Dangerous viral challenges and direct messaging features can be exploited by predators.	
Snapchat	• Disappearing messages encourage risky behaviour and make monitoring difficult. • Snap Map reveals real-time location unless disabled, increasing vulnerability.	
Instagram / Threads	• Exposure to adult content, body image pressures, and contact from strangers via DMs (direct messages). • Public profiles and filters can affect self-esteem and increase risk of exploitation.	
Discord	• Unmoderated chatrooms and servers can contain explicit content and grooming risks. • Children may be exposed to cyberbullying or inappropriate conversations.	
Roblox	• In-game chat and user-generated content can include adult themes or grooming tactics. • "Free Robux" scams and private messaging are used to manipulate children.	
OmeTV / Monkey / *Similar video chat apps*	• Anonymous video chats with strangers often lead to exposure to sexual content. • No registration required, making it easy for predators to connect with children. • These apps change frequently or get rebranded	
Telegram	• Encrypted and disappearing messages make monitoring difficult. • Public channels may share adult or extremist content.	

BeReal	• Real-time photo sharing can reveal location and personal routines. • Minimal moderation increases risk of oversharing and exposure.	
Triller	• Weak age restrictions and less moderation than TikTok. • Children may be exposed to explicit videos and unsafe interactions.	
Skout / MeetMe / Badoo	• Location-based dating apps that allow children to connect with strangers. • Fake age profiles and GPS tracking increase risk of exploitation.	
YouNow / ChatRoulette *and similar*	• Live streaming and random video chats can lead to inappropriate exposure. • Children may unknowingly share personal information with anonymous viewers.	
YUBO	• Often used to meet strangers, with weak age verification. • Location sharing is integral, increasing risk of grooming and exploitation.	



Tools and Technologies Children May Use to Hide Online Activity		
Calculator Vault Apps	• Disguised apps used to hide photos, videos or messages from parents. • Often appear as a standard calculator app icon. • Commonly used to conceal sexting or other inappropriate content. • Example: 'Calculator%'	
VPNs	• Can bypass age restrictions, allowing children to access pornography and other inappropriate material. • Mask browsing activity, making it harder for parents or professionals to monitor use or intervene early. • May enable access to unsafe platforms or contact with others without safeguards in place.	
AI Chatbots	• UK safeguarding bodies have flagged apps like Replika, Character.AI, Nomi and Snapchat's "My AI" due to their potential to facilitate harmful roleplay, boundary-blurring interactions and emotional dependency. • Some chatbots can bypass or inadequately enforce age restrictions and have been reported to engage in inappropriate or sexualised conversations. • There are concerns about children forming emotional attachments to chatbots that simulate affection or romantic interest, which may distort their understanding of relationships and consent.	 
Resources: NSPCC, Ofcom, Internet Matters, Children's Commissioner for England, UK Government		

Helpful Resources to Explore

These resources can support your understanding of online safety and offer practical advice for keeping children safe in the digital world.

- iwf.org.uk/
- ncsc.gov.uk/collection/top-tips-for-staying-secure-online
- ceopeducation.co.uk/parents/ask-the-awkward/
- nspcc.org.uk/keeping-children-safe/online-safety
- saferinternet.org.uk/guide-and-resource/parents-and-carers
- shorespace.org.uk (for teenagers)

Glossary

This glossary explains key terms used throughout the guide to support carers in understanding online safety tools and risks.

Active Monitoring
Using apps or tools to regularly check what a child is doing online — such as browsing history, messages, or social media activity. It should be done openly and explained to the child as a safety measure.

Age-Appropriate Content
Online material that is suitable for a child's age and maturity level. This helps protect children from content that may be harmful, confusing, or upsetting.

Algorithm
A set of rules used by apps and websites to decide what content to show a user. Algorithms can quickly expose children to harmful or inappropriate material based on what they've clicked or watched before.

App Permissions
Settings that control what an app can access on a device — like the camera, microphone, location, or contacts. Limiting permissions helps protect privacy and safety.

Apple Screen Time
A built-in tool on Apple devices that lets carers set limits on screen time, block apps, and monitor usage.

Child Profiles
Special user accounts designed for children that restrict access to certain apps, websites, or features. These help create a safer digital environment.

Content Filtering Software
Apps or tools that block or hide inappropriate content (like adult material or violence) based on a child's age or needs.

Cyberbullying
Bullying that happens online — through messages, social media, or games. It can include name-calling, threats, or spreading rumours and can be very harmful to a child's wellbeing.

Device-Free Zones
Times or places where devices are not used — such as during meals, bedtime, or school. These help promote healthy habits and reduce screen time.

Digital Use Contract / Agreement / Safety Plan
An agreement between carers and children about how devices and the internet will be used. It can include rules, boundaries, and consequences and should be age-appropriate and reviewed regularly.

Disappearing Messages
Messages that automatically delete after being read or after a short time. These can make it harder for carers to monitor conversations and may encourage risky behaviour.

DM (Direct Message)
A private message sent between users on social media platforms. Unlike public posts or comments, DMs allow one-to-one conversations that are not visible to others.

Encrypted Messages
Messages that are scrambled so only the sender and receiver can read them. While this protects privacy, it can also make it difficult to monitor for safety concerns.

Google Family Link
A free app from Google that helps carers manage a child's device — including screen time, app approvals, and location tracking.

GPS Tracking
Technology that shows where a device (and its user) is located. It can help carers know where a child is, but also raises privacy concerns if misused.

Grooming
When someone builds a relationship with a child online to trick or manipulate them — often with the aim of abuse or exploitation. Grooming can happen through games, social media, or messaging apps.

High Restriction
A very strict level of control over a child's device — such as locking it down to only approved apps, disabling app stores, or requiring parental approval for every action. Often used when there are serious safety concerns.

Inappropriate Content
Material that is not suitable for children — such as sexual content, violence, or hate speech. It can be upsetting or harmful to view.

Kiosk Mode
A setting that locks a device so only approved apps or features can be used. It's often used to create a very restricted and safe digital space for children.

Location Sharing
When a device or app shows where the user is in real time. This can be risky if strangers or unsafe contacts can see the child's location.

Live Streaming
Broadcasting video in real time, often to strangers. Children may accidentally share personal information or be exposed to inappropriate content.

Microsoft Family Safety
A free tool from Microsoft that helps carers manage screen time, filter content, and track location across Windows and Android devices.

Monitoring Tools
Apps or settings that help carers keep track of a child's online activity — including what they're doing, who they're talking to, and what content they're accessing.

Online Exploitation
When someone uses the internet to take advantage of a child — often for sexual, emotional, or financial reasons. It can happen through manipulation, threats, or trickery.

Parental Controls
Settings or apps that help carers manage what children can do on devices — such as blocking websites, limiting screen time, or approving app downloads.

Privacy Settings
Controls that decide who can see a child's posts, messages, or personal information online. These should be set to private to protect children from strangers.

Remote Lock or Wipe
A feature that lets carers lock or erase a device from a distance — useful if a device is lost, stolen, or being misused.

Safe Search Filters
Settings that block inappropriate content from appearing in search results — useful on browsers and platforms like YouTube.

Screen Time Reports
Summaries that show how much time a child spends on their device and which apps they use. These help carers understand usage patterns and set limits.

Soft Monitoring
A gentle approach to monitoring a child's online activity using tools like parental controls or screen time apps. It's less intrusive than active monitoring and focuses on guidance and support rather than strict oversight.

VPN (Virtual Private Network)
A VPN is a tool that hides what someone is doing online by creating a private, secure connection. Children may use VPNs to bypass parental controls, access blocked websites (including adult content), or hide their browsing history. This makes it harder for carers to monitor online activity or step in early if something goes wrong. If a child is using a VPN, it's important to talk with them about why and to review safety settings together.

