Navigating the Digital World

A Parent's Essential Guide to Online Safety, AI, and Healthy Digital Habits



Introduction

2Simple, creators of Purple Mash, have put together this informative guide to help you to enable your child to grow into a responsible digital citizen who can stay safe while getting the most out of the digital world.

Keeping up with online technology can feel overwhelming. Today's children are growing up with social media, apps, and artificial intelligence in ways earlier generations never experienced. While this fast pace can feel worrying, technology isn't something to fear. When used with care, it gives children fantastic ways to learn, play, and create.

The tips and advice in this section are designed to be flexible and easily adaptable to meet your child's unique needs, including those with Special Educational Needs (SEN). While a wide variety of excellent online resources are available to support children with diverse learning needs, Childnet International serves as an ideal starting point by offering helpful tools and direct connections to other trusted providers of free advice and support.

https://www.childnet.com/resources/know-it-all-for-teachers-sen

Getting Involved, Setting Examples & Talking Openly

Simply blocking everything rarely works. A much better approach is exploring apps and games together so you understand what your child is doing and can guide them safely. Children also copy how adults use devices, so setting simple family rules - like no phones at the dinner table and treating others politely online - creates healthy habits early on.

Parental control filters and safety settings are helpful first steps, but no software or app block is 100% foolproof. Your strongest safety tool is an open, calm relationship. Your child needs to feel confident coming to you if they make a mistake or see something upsetting online, knowing you won't get angry or take their device away.

Together, these simple principles will help your family feel confident, safe, and supported in today's digital world.



45%

*of children **aged 8–17** in the UK have been exposed to some form of harmful content online*

(Children's Commissioner 2022)

Policy & Safeguarding: The UK Online Safety Act & Social Media Ban

The Online Safety Act is a UK law that makes tech companies and search engines legally responsible for keeping children safe online. Under this law, companies must quickly take down illegal content, properly check users' ages, and adjust the automated systems that recommend posts and videos. This prevents children from being repeatedly shown dangerous content about self-harm, eating disorders, cyberbullying, or grooming. Ofcom (the official UK regulator) monitors compliance and can hand out heavy fines to tech platforms that fail to protect young users.

The Proposed Under-16 Social Media Ban

Even though most social media platforms officially require users to be at least 13, many primary school children still manage to set up profiles. To tackle this, the UK government has proposed banning social media access for anyone under 16. This change would require apps to strictly verify a person's age before letting them join, supporting phone-free rules in schools across England. However, parents still need to watch out for common workarounds - such as children using secret secondary accounts, unmonitored messaging apps, or VPNs (privacy tools that bypass network blocks) to stay connected with friends.

Practical Guidance for Parents

Legislation: creates a safer framework, but rules alone cannot replace home guidance.

Explain Age Limits: Focus on why restrictions exist, protecting mental health and privacy rather than imposing arbitrary bans.

Maintain Open Communication: Reassure children they can report upsetting content or mistakes without fear of judgment or losing device access.

Audit Settings Together: Regularly review device privacy, location sharing, and app permissions.

*Despite most platforms having a minimum age of **13, six in ten children** aged **8 to 12** who use them are signed up with their own profile.*

(OFCOM 2024)

Need more support? Contact us:
Call: 020 8203 1781 | Email: support@2simple.com | Visit: help.2simple.com

Self-Image and Identity: Avatars, Filters, and Deepfakes
Visual Filters & AI Avatars

Children love creating digital characters (avatars) and using photo filters in games and apps. While making custom characters can be a fun way to express creativity, AI beauty filters and picture-perfect avatars can quietly change how children view themselves. Over time, seeing these flawless images can create unrealistic expectations about physical appearance, damaging a child's natural self-confidence from an early age.

Deepfakes & Fake Images

Modern AI tools make it easy for anyone to edit photos or create "deepfakes" - fake videos, audio clips, or pictures that look surprisingly real - using just a few uploaded photos. Primary school children need to learn that what they see on a screen can easily be edited or completely made up. Teaching them this helps them understand why it's important to keep personal photos private and to remember that online pictures are rarely untouched.

Practical Guidance for Parents

Promote Authenticity: Encourage children to value their real-world self over online curation, discussing how digital images are frequently filtered or AI-enhanced.

Limit Photo Sharing: Teach children not to post clear facial photos or personal media publicly where they could be scraped or manipulated by AI tools.

Discuss Online vs. Reality: Talk openly about how algorithms promote idealised body images, helping children build emotional resilience against peer comparison.

1 in 5

children aged **8-15** *spends three to four hours a day on an internet enabled device.*

(The Guardian, April 2025)



Need more support? Contact us:
Call: 020 8203 1781 | Email: support@2simple.com | Visit: help.2simple.com

purple mash

Online Relationships & The Under-16 Social Media Ban
Online Friendships & Peer Pressure

Children love using apps and games to chat with friends, play together, and feel part of a group. However, the strong desire to fit in can make them want to bypass age limits or school phone rules. As rules around social media change, it's vital to help your child understand the difference between healthy, supportive friendships and risky or pressure-filled chats.

AI Chatbots & Virtual Friends

Computer-generated chatbots and AI companions are now built into many messaging apps, search tools, and online games. Because these AI tools reply instantly and sound friendly, young children can easily mistake them for real friends or trusted confidants. This can lead to children sharing personal secrets, relying emotionally on a computer program, or being exposed to unmonitored chats without parents knowing.

Practical Guidance for Parents

Establish Chat Boundaries: Remind children that online contacts, including AI chatbots, are not real-world friends, and private information should never be shared.

Monitor Group Messaging: Set clear guidelines on messaging etiquette, blocking strangers, and managing group chat volume to prevent social overload.

Encourage Offline Connection: Support face-to-face playdates and hobbies so children do not rely solely on digital channels for friendship and belonging.



35%

of children accepted a friend request online from someone they did not know.

(Crime Survey for England and Wales, 2024)

Need more support? Contact us:
Call: 020 8203 1781 | Email: support@2simple.com | Visit: help.2simple.com

Online Reputation & Digital Footprints in the AI Age, Understanding Digital Footprints & 'Sharenting'

Every photo, video, comment, and account registration shared online creates a permanent digital footprint - a lasting trail of information. Parents often start this digital footprint for their children through 'sharenting' (posting photos, school updates, or milestones on social media). As primary school children start making their own posts and accounts, helping them understand that what goes online stays online helps protect their future privacy and reputation.

AI Photo Scraping & Privacy Risks

Public photos and posts can now be automatically collected by AI systems to train image tools or feed facial recognition databases. Photos shared online today could easily be saved, searched, or repurposed by AI algorithms years into the future. Keeping account settings strictly private and being thoughtful about sharing photos online are simple, crucial steps to protect your child's digital identity.

Practical Guidance for Parents

Ask for Consent: Seek your child's permission before sharing their photos online, modelling respect for their digital footprint from an early age.

Tighten Account Privacy: Ensure family photo-sharing accounts, blogs, and social profiles are restricted strictly to verified friends and family.

Teach the 'Billboard Rule': Remind children that anything posted digitally can be saved or forwarded, so they should only share content they would be comfortable seeing on a public billboard.



Online Bullying, Wellbeing and AI-Assisted Harassment

24/7 Cyberbullying & School Support

Unlike traditional bullying that stops when the school day ends, cyberbullying follows children directly into the home through their screens, making it feel non-stop. In primary schools, online bullying often happens in class group chats, online gaming lobbies, or through leaving children out of group chats. Watch for small changes in your child - such as sudden mood swings, trouble sleeping, nervousness when their phone buzzes, or suddenly avoiding their device. Talking to your child's school and using official UK reporting services like CEOP (Child Exploitation and Online Protection) helps you get support quickly.

AI-Generated Bullying & Fake Profiles

New AI tools make it easy for anyone to create harmful fake images, copy someone's voice, or set up fake profiles to pick on or impersonate classmates. Children must understand that making or sharing fake AI images or messages to target others is a serious form of bullying that schools and police take very seriously. Most importantly, if your child is ever targeted by fake photos or online bullying, reassure them that they are never to blame and that you are there to help.

Practical Guidance for Parents

Save Evidence First: Advise children not to delete abusive messages or synthetic images; take screenshots, block the accounts, and report the content to the platform.

Inform School Safeguarding: Contact your child's school and ask for the Designated Safeguarding Lead (DSL) if harassment involves peers or affects their wellbeing at school.

Offer Unconditional Support: Reassure your child that coming forward with concerns will lead to support and solutions - not immediate punishment or device confiscation.

7,000

Sexual Communication with a Child offences were recorded by police last year (2023/24) – up

89%

since 2017/18 when the offence first came into force.

(NSPCC 2024)

Managing Online Information & Developing Scepticism Spotting Fake Media & Asking Questions

In a world with smart computer tools, seeing or hearing is no longer believing. Children often come across fake photos, edited videos, or computer-generated voice clips while browsing video feeds or playing games. Teaching your child to ask simple questions - like *"Who made this?"* and *"Is this real or edited?"* - helps them learn to question what they see online instead of believing everything right away.

When AI Makes Things Up ("Hallucinations")

AI search tools and chatbots answer questions very confidently, but they frequently make mistakes or invent false details (sometimes called AI "hallucinations"). Children need to know that AI chatbots are not magical or always correct. Encouraging your child to double-check facts using trusted websites, school textbooks, or asking a teacher is a crucial skill for schoolwork and research.

Practical Guidance for Parents

Teach the 'Three-Source Rule': Encourage children to verify news, facts, or shocking images across three reliable, independent websites before accepting or sharing them.

Spot AI Artefacts: Help children identify common signs of synthetic media, such as unnatural hand shapes, distorted background details, or robotic voice phrasing.



Question Algorithmic Recommendations: Discuss how video feeds and search algorithms prioritise engaging or sensational material over balanced, factual information.

Need more support? Contact us:
Call: 020 8203 1781 | Email: support@2simple.com | Visit: help.2simple.com

Health, Wellbeing and Lifestyle: Balancing Screen Time & Tech Apps Designed to Keep Children Hooked

Popular games, social apps, and video platforms are specially built with features like autoplay, endless scrolling, and pop-up alerts to keep children watching for as long as possible. Because primary school children are still developing self-control, turning off a screen or stopping a game can easily lead to frustration, arguments, and family stress.

Protecting Sleep, Health & Active Play

Using screens late at night or for hours on end can disrupt your child's sleep, strain their eyes, and lead to less physical activity. The bright light from phones, tablets, and TVs tricks young brains into staying awake, while fast-paced games and videos make it hard to calm down. Setting screen-free areas (like bedrooms) and turning off devices at least an hour before bedtime helps ensure your child gets a good night's rest.

Practical Guidance for Parents

Establish Tech-Free Zones: Keep bedrooms, mealtimes, and family discussions entirely screen-free to protect restful sleep and face-to-face communication.

Use Physical Visual Timers: Give primary-aged children clear countdowns or physical timers before screen time ends, reducing resistance when turning off devices.

Balance Digital & Offline Activities: Encourage daily physical play, outdoor exploration, and hands-on creative hobbies to build a healthy, well-rounded routine.



Need more support? Contact us:
Call: 020 8203 1781 | Email: support@2simple.com | Visit: help.2simple.com

Privacy, Security and Data Harvesting by AI Smart Devices and Data Collection

Smart devices, connected toys, and AI apps rely on gathering personal information to work. From voice recordings and location tracking to chat histories, details about how your child uses apps are constantly gathered. Parents should know that many apps and AI tools save this information to show targeted ads or to help train their computer systems.

Home Wi-Fi & Simple Security Steps

Keeping your child's information safe starts at home. Simple actions - like turning on free parental controls through your home Wi-Fi provider (such as BT, Sky, or Virgin Media), turning off location sharing in app settings, and keeping passwords private - help block unwanted tracking and protect your family's devices.

Practical Guidance for Parents

Audit App Permissions: Regularly check device settings to revoke unnecessary camera, microphone, and precise location access for everyday apps.

Opt Out of AI Training: Review privacy toggles within generative AI apps and platforms to opt out of having your child's prompts and data used for model training.

Secure Home Devices: Set strong passwords and two-factor authentication on smart speakers, gaming consoles, and routers, switching off listening features when idle.

32%

of parents surveyed in the UK said that their child uses social media independently.

(OFCOM 2024)

Copyright, Ownership and AI Homework Tools
AI Homework Tools & Doing Their Own Work

Smart AI chatbots can instantly write stories, solve maths problems, or answer homework questions. While these tools can be great for explaining tricky topics or brainstorming ideas, using them to complete assignments directly stops children from learning for themselves and breaks school rules. Children need to learn that AI is a helpful study partner, not a shortcut to avoid doing their own thinking.

AI Pictures, Music & Giving Credit

AI tools create images, music, and text by scanning millions of real creations made by human artists, writers, and musicians. Because AI builds on other people's work, it's important for children to understand that AI-generated pictures or text aren't entirely original. Teaching children to give credit when they use AI for school projects helps them respect human creativity and learn fair use from an early age.

Practical Guidance for Parents

AI Homework Rules: Agree on clear guidelines with your child on when AI can be used (e.g., brainstorming or explaining a tough concept) versus when work must be entirely their own.

Teach Source Attribution: Encourage children to cite or acknowledge when they have used digital references or AI assistance in their school projects.

Question Algorithmic Recommendations: Discuss how video feeds and search algorithms prioritise engaging or sensational material over balanced, factual information.

Nearly 1 in 3 parents (32%)

report that their young children navigate the internet independently without active parental filtering or supervision enabled on their devices.

(OFCOM 2024)

Getting to Grips with Devices, Software & AI Safety Settings Setting Up Free Broadband & Device Safety Controls

Parental controls work best when set up right at home. Major UK internet providers (like BT, Sky, Virgin Media, and TalkTalk) offer free family filters that automatically block adult or risky content across every device connected to your home Wi-Fi. In addition, built-in safety tools - such as Apple Family Sharing, Google Family Link, and settings on gaming consoles (PlayStation, Xbox, Nintendo Switch) - let you set age limits on apps, block unexpected in-app spending, set daily screen limits, and check what games your child is playing.

Checking App Settings & Turning Off AI Features

Many popular apps, messaging services, and search engines now automatically include built-in AI chatbots. It is a good habit to regularly check app settings with your child to turn off unwanted AI features, turn off location sharing, and stop apps from saving personal chat messages or uploaded family photos.

Practical Guidance for Parents

Filter at the Router Level: Activate your UK ISP's family filters to ensure automatic baseline protection for smartphones, tablets, and smart TVs at home.

Lock Down Payments: Disable one-click store purchases, require password authorisation for downloads, and set up spending limits on gaming accounts.

Review Settings with Your Child: Walk through privacy toggles together so your child understands that safety controls are designed to protect them, not restrict their independence.



Need more support? Contact us:
Call: 020 8203 1781 | Email: support@2simple.com | Visit: help.2simple.com

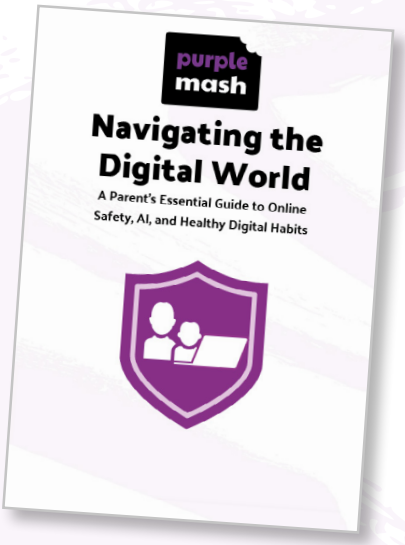
purple mash

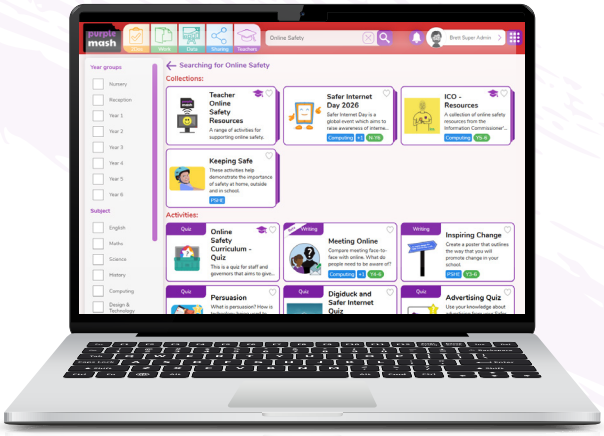
3 Steps
to supporting your child, online safety at home

Read this handy guide

(You're already doing a great job)

1





2

Try online safety activities

Log in to Purple Mash with your child and search 'Online Safety' to try fun activities at home. Home access is free if your child's school subscribes to Purple Mash.

Get a free trial

Don't have Purple Mash yet? Get a free home access trial now at www.2simple.com. A 1 year home access account is less than £5 a month and it includes 1,000s of educational games and activities to keep your children busy!

3

purple mash

Start my trail now

Need more support? Contact us:
Call: 020 8203 1781 | Email: support@2simple.com | Visit: help.2simple.com

purple mash

Jargon Buster: From Algorithms to AI

A concise glossary blending essential foundational concepts with modern terms every parent in England should know:

Adware

An application that displays adverts and may redirect searches.

AI Hallucination

When a generative AI tool creates false or fabricated information while presenting it as fact with confidence.

CEOP (Child Exploitation and Online Protection)

A command of the UK National Crime Agency that works to protect children from sexual abuse and grooming online.

Circumventor Sites

Websites or proxy services used to bypass network filters and content restrictions.

Cyberbullying

The use of electronic communication to bully.

Deepfakes & Synthetic Media

Hyper-realistic images, videos, or voice clones created or altered using generative AI software.

Emoji

A digital image used to express an idea, action or emotion.

Age Assurance / Verification

Technical methods used by platforms to confirm a user's age before granting access to age-restricted content or social features.

Bot

A program that does things without users' instructions. Many bots are malware.

Chatroom

A place where online users can chat.

Cookie

A small file which records a user's personal preferences.

Decoy App

These apps help children hide videos/ images from their parents.

Digital Footprint

The permanent trail of data, searches, and posts left behind through online activity.

Education for a Connected World (EfCW)

The UK framework outlining the digital safety skills and citizenship children should learn across primary education.

Need more support? Contact us:
Call: 020 8203 1781 | Email: support@2simple.com | Visit: help.2simple.com

purple mash

Firewall

A system which protects a network from external threats.

Generative AI & LLMs (Large Language Models)

AI tools capable of generating new text, images, code, or audio based on user prompts

Grooming

Someone who gains a child's trust for sexual exploitation or trafficking.

Identity Theft

A crime in which personal information is used or pieced together for financial gain.

In-app Purchasing

Buying services or products within apps, which may be billed to phone accounts or linked cards.

ISP (Internet Service Provider)

An internet service provider gives access to the internet.

Malware & Spyware

Unauthorised software designed to damage, disrupt, or covertly gather data from a device.

Fabotage

Unauthorised changes to another user's social media account or content without permission.

Gamer Tag

An alternate identity created for online gaming.

Griefer

Someone who deliberately harasses online gamers

Hacker

A person who gains unauthorised access to information.

IM (Instant Message)

Real-time online text messaging between two or more users over the internet.

Incognito Browsing

Users can browse the web without their history being recorded on a device.

Netiquette

The standard code of polite, respectful, and responsible behaviour online.

PEGI Ratings

Pan European Game Information age ratings designed to guide parents on the content suitability of video games and apps.

Pharming

Redirecting users to fake websites to steal personal information.

Photosharing

Apps and sites allowing users to share photos; this can be very damaging for children.

Selfie

Self-portrait photo uploaded online.

Sharenting

The practice of parents posting photos, videos, or details about their children on social media platforms.

Spam

Messages sent to user for phishing, malware and advertising purposes.

Troll

A user who posts inflammatory messages.

Video Hosting Sites

Online services which allow users to post and view clips.

Phishing

Fraudulent messages or emails designed to trick users into revealing confidential personal data.

Profile

A profile users have created for social media accounts.

Sexting

Sending or receiving sexually explicit messages, images, or videos.

Social Media

The sharing of content and participation in social networking.

Trojan

Malicious software disguised as legitimate programs.

UK Online Safety Act

Legislation placing a strict legal duty of care on tech platforms to protect children from harmful and illegal content.

Virus

A harmful program capable of replicating itself and damaging systems.