Do Your PART

Remember these key steps to Do Your PART:

- **Protect**: Enable parental controls on devices, set strong passwords, and review privacy settings.
- Advise: Talk to your children about the importance of online safety, emphasising responsible sharing and the risks of oversharing.
- **Report**: Encourage open communication so they feel comfortable reporting anything that makes them feel uneasy.
- **Teach**: Show them how to recognise phishing attempts, secure their accounts, and spot inappropriate content.

Protect

Security and Parental Settings.

Use the parental control settings on your devices to restrict access to inappropriate content. Take time before gifting to understand how this can be done – we know that it's a lot harder to set this up when you have an excited child on your hands.

Follow step-by-step guides to set up parental controls on your smartphone or tablet. <u>NSPCC</u>: Offers comprehensive advice on setting up parental controls to keep children safe online. They provide guidance on managing content filters, screen time, and privacy settings.

Wi-Fi Security.

Enable content filters on your home Wi-Fi to block adult content.

Many ISPs (Internet Service Providers) implement safety restrictions at the network level when setting up home internet. These restrictions are designed to block access to potentially harmful or inappropriate content; however, checks need to be done with individual suppliers to understand the level to which this has been done. Parents can check with their provider or via websites such as <u>Internet Matters Network</u>, which offers comprehensive guides on setting up parental controls for various ISPs, including step-by-step videos and visual instruction.

Please be aware that further controls can be applied to devices themselves and at game or app level, and that wi-fi restrictions will not operate if children are using their devices on mobile data – these need to be set up separately.

Parental Control Options – Devices.

Remember that devices have content filters built in that require set up, which can include time management settings, for example on SMART TV's that can manage what your child can watch/access.

Platform Guidelines.

There are privacy and data sharing policies of online platforms, apps and games, as well as recommended age limits. These can help you understand how your child's data is used. Age limits are applied for a reason and are not just limited to data protection. Age limits aims to protect children from risks such as cyberbullying, exposure to inappropriate content, and online harms.

Group messaging such as WhatsApp is a great way to keep in touch with multiple friends, however, they can quickly turn into a headache when the messages start piling up. Parents need to be aware of all features such as location sharing, and chat lock which will remove a chat thread from the app's regular onscreen inbox and place it into a new folder that can only be opened by a password or biometric, such as facial recognition or a fingerprint.

Internet Matters has step-by-step guides to support users and outline key functions. Internet Matters Social Media Settings

Advise

Managing Screen Time.

Set a daily screen time limit for recreational use on all devices. Set realistic and flexible screen time schedules that account for school, leisure, and family activities. We recognise that every family and child is different, and parents will know how device usage impacts their own child, so set goals and limits that are realistic and workable for you. Children could be asked to contribute to what they think is fair.

Encourage the use of apps with educational value, and balance screen use with physical play and outdoor activities. Know what works for your child, and what impacts their mood and wellbeing. You can use screen time management apps to set reminders for breaks.

We know that our children will role model what they see, so it may be that we need to be mindful of our own device use, no matter how difficult that can be!

Report

Agree on Family Device Usage.

Be clear on rules from the outset. Ideas include creating a family charging station in a common area to keep devices out of bedrooms and non-shared areas and drafting a family agreement to ensure everyone's on the same page regarding device usage. Commonsense Media and Internet Matters both have contract templates to download. <u>Commonsense Media</u> <u>Device Contract</u>.

Open Communication.

Regularly ask your child about their online activities and friends. We know that they will love to tell you about their latest Roblox or Minecraft adventures! Fostering open and honest conversations about online usage allows interests to be shared and for children to understand the many positives of online life as well as the pitfalls. Encourage co-viewing of online content to discuss and understand their interests and discuss the content.

Discuss acceptable online behaviour with your children, emphasising kindness and respect in digital interactions. Arm them with knowledge of how to mute groups, leave and to share worries with you. Make sure your children know they can come to you with any concerns about their online experiences without fear of punishment.

For older children, talk about consent, the sharing of images and how to report and get help.

CEOP – Think You Know has information on this, online sexual harassment, healthy relationships and more.<u>11-18s | CEOP Education</u>. They also have information for younger children as well as professionals, parents and carers.

Use shared accounts for younger children to keep tabs on their activity, and schedule regular check-ins to discuss any concerns or questions.

Teach

Health.

Promote a healthy balance of on and offline activity – with the understanding that our children's lives are different to ours with much of their socialisation online.

Keep devices out of bedrooms overnight to promote better sleep habits. Explain to children how device activity before bed can hinder their sleep.

Start Early.

Preschoolers: Begin with basic concepts like not talking to strangers online and asking for permission before using devices.

Primary KS1: Introduce the idea of personal information and why it should be kept private. Use simple language to explain the risks.

Tweens and Teens: Discuss more complex topics such as cyberbullying, online predators, and the importance of a positive digital footprint.

Use Real-Life Scenarios.

Role-play situations where your child might encounter a stranger online or receive a suspicious message. Discuss how they should respond. Teach Critical Thinking. Encourage your children to question the authenticity of online information and to think before they click on links or share personal details.

Parental Advice Websites for Online Safety and Device Setup

NSPCC - Offers comprehensive advice on setting up parental controls and keeping children safe online. Keeping children safe online | NSPCC

Internet Matters - Provides detailed guides and resources for setting up parental controls on various devices and platforms. <u>Keep Children Safe Online: Information</u>, <u>Advice, Support - Internet Matters</u>

UK Safer Internet Centre - Offers a parents' guide to technology, including safety tools and advice for responsible use. <u>Homepage - UK Safer Internet Centre</u> CEOP - **The National Crime Agency's CEOP Education team.** <u>CEOP Education</u>

Common Sense Media - Is an independent voice for kids, families, and communities everywhere. They combine original research with game-changing advocacy efforts to make the digital world work better for all kids. <u>Common Sense Media: Age-Based Media</u> <u>Reviews for Families | Common Sense Media</u>