New Devices, New Rules:
A Parent's Essential Online Safety Checklist

Dear Parents and Carers,

As the Christmas holidays approach, many of our children and young people will be excitedly unwrapping new phones, tablets, gaming consoles, or virtual reality headsets.

This is a wonderful opportunity for learning, connecting, and fun! However, new devices and increased time online also mean a change in routine and, potentially, an increase in digital risks.

To help you ensure the festive season remains safe and positive, we've teamed up with our marketing and online safety partners, Mitchell Digital Media Ltd, to provide this simple, actionable checklist.

By taking just 15 minutes to follow these steps, you can set a safe, secure foundation for the year ahead.

Part 1: Setting Up for Success (*Before They Log On*)

This is the most crucial step. Whenever possible, set up the device *before* giving it to your child.

1. **Activate Parental Controls (Device Level)**
    a. These filters are your first line of defence, allowing you to manage screen time, block unsuitable content, and prevent accidental in-app purchases.
    b. Check the device's main settings: **Apple** uses **Screen Time**. **Android/Google** uses **Family Link**. **Microsoft** uses **Family Safety**.

2. **Restrict In-App Purchases**
    a. Avoid a costly bill shock! Most games and apps make it easy for children to spend real money.
    b. Go into the device settings and disable in-app purchases, or require a secure password *known only to you*.

3. **Turn Off Location Services**
    a. Sharing a child's location can inadvertently compromise their safety and privacy.
    b. In the device settings, turn off **Location Services** for social media and general apps. Only allow it for essential tools like maps (with discretion).

4. **Check the Network Controls**
    a. Your home broadband router (e.g., Sky, BT, Virgin Media) often has free filters you can activate to protect *all* devices connected to your Wi-Fi.
    b. Visit your broadband provider's website and look for their 'security' or 'parental controls' section

---

Part 2: The Essential Family Conversation

Technology changes, but the need for open communication does not. Sit down with your child and agree on your family's digital rules.

Focus Area 1: Privacy and Personal Information

- **The School Name Rule:** Remind your child **never** to share personal information online, including their address, phone number, or the **name of our school** or their **form tutor**, in posts, profiles, or chats with strangers.
- **The Digital Footprint:** Explain that everything they post, share, or 'like' leaves a permanent record (a 'digital footprint'). Encourage them to pause and think: *"Would I be happy for my Headteacher, my grandma, or a future employer to see this?"*
- **Privacy Settings:** Use the device together to set all social media and gaming profiles to **Private** or **Friends Only**. Limit who can tag them in photos or contact them via direct message.

Focus Area 2: The 'Worry' Rule

- **Be Curious, Not Furious:** Make a pact that if they see something that worries, scares, or upsets them online, they can come straight to you without fear of getting in trouble or having their device taken away.
- **The Block and Report Rule:** Teach them how to use the 'Block' and 'Report' functions on apps and games. This is their power tool to manage their own safety.
- **Age Matters:** Discuss the minimum age requirements (usually **13+**) for platforms like Instagram, TikTok, and Snapchat. These limits exist for safeguarding reasons.

Part 3: Useful UK Online Safety Resources

If you need detailed, step-by-step guidance on setting controls for specific platforms, these UK-based sites are your best friends:

- **Internet Matters:** Provides age-specific advice and step-by-step guides for most devices and apps.
- **NSPCC Keeping Children Safe Online:** Reviews of the latest apps, games, and social media sites to help you understand the risks.
- **Childnet:** Fantastic resources, including a template for creating a **Family Agreement** for technology use.
- **CEOP (Child Exploitation and Online Protection Centre):** The police's central resource for reporting online sexual abuse or inappropriate contact.

We wish you and your family a safe, happy, and digitally sensible Christmas break. We look forward to seeing everyone return safe and ready to learn in the New Year.