

St Bede's Online Safety Newsletter



St Bede's On-line Safety Newsletter: Keeping Our Children Safe Online

Welcome to our latest On-line Safety newsletter! As technology evolves, so do the challenges of keeping our children safe in the digital world. This edition focuses on key areas to help you manage your child's online experiences at home.

Current Key Concern: The Online Safety Act and Harmful Content

The new **Online Safety Act (2023)** is now being enforced, placing new legal duties on social media companies and other online platforms to protect children.

What you need to know:



- **Protecting Children from Harm:** Platforms must now use highly effective **age assurance** (age checks) to prevent children from seeing the most harmful content, such as material relating to **pornography, suicide, self-harm, or eating disorders**.
- **What this means for you:** Even with these new laws, our children may still encounter age-inappropriate or distressing content by accident. It is vital to continue the conversation at home.

☒ **Action for Parents:** Talk to your child regularly about what they do and see online. Reassure them that they can tell you, or a trusted adult, about anything that makes them feel scared, worried, or uncomfortable.



Online Relationships: Friends Old and New

For primary children, online relationships often start in games (like Minecraft or Roblox) or on shared family devices. It's important to discuss the nature of these connections, as the same rules for good friendship apply online as they do in the playground. In School we have been talking across the school about Online Relationships and encouraging the children to speak with a trusted adult.

 The Positives of Online Connections	 The Negatives and Risks
Connecting Over Interests: Your child can meet others who love the same niche games, books, or hobbies, which can boost their sense of belonging.	People Pretend to be Someone Else: Online strangers might lie about their age, name, or gender. This is known as <i>deception</i> and can be very dangerous.
Communication Practice: Typing and chatting online helps children learn to express themselves clearly and practice writing skills.	Cyberbullying: Being mean online can be easier for some children as they don't see the person's reaction. It's vital they know how to block, report, and tell an adult.
Keeping in Touch: It allows children to keep up with friends or family who live far away or that they don't see every day.	Pressure and Secrets: Strangers or even 'friends' might pressure your child to share private photos or personal information. They must know to NEVER share private details.

Top Tip for Parents: Encourage your child to only communicate with people they already know in real life. If they are talking to a new online friend, they should keep the chat public within the game or site, never moving to a private message app without your permission.



⚙️ Parental Controls: Your Digital Safety Net

Parental controls are a valuable tool for supporting the boundaries you set. They are your technical defence against inappropriate content and excessive screen time.

1. Managing Time and Content

Parental controls are available in three key areas:

- **Internet/Broadband Provider:** Your home router can often apply content filters across all devices connected to your Wi-Fi (e.g., BT, Sky, Virgin Media filters). This is your first line of defence.
- **Device Settings:** Smartphones, tablets (iPad, Android), and computers have built-in controls (like **Apple Screen Time** or **Google Family Link**).
 - **Time Limits:** Set daily usage limits for the whole device or specific apps. You can also schedule **Downtime** (e.g., stopping access after 8 pm).
 - **Content Filtering:** Restrict access to age-inappropriate websites or filter apps and games based on their PEGI/age rating.
- **App/Game Settings:** Individual services (like Netflix, YouTube Kids, or gaming consoles like Xbox/PlayStation) have their own safety settings to limit age ratings, chat, and spending.

Crucial Step: When setting up controls, always set a **Passcode** that only you know to prevent your child from easily changing the settings.

2. Block and Report: Teaching Your Child to Take Control

Teach your child the key rules for dealing with anything that makes them feel uncomfortable, sad, or scared online.

Action	What It Means	When to Use It
Block	Stops a person from being able to contact or interact with your child again.	If someone is being unkind, bullying, or is a stranger who won't leave your child alone.
Report	Sends a message to the platform (game or social media site) administrators.	If someone is bullying, sharing illegal or harmful content, or pretending to be someone else.
Tell	Always tell a trusted adult! (Parent, teacher, relative).	This is the most important step. If they see or receive something worrying, they must tell an adult immediately.

Key Message: Remind your child that blocking or reporting someone is **not their fault** and it is the right thing to do to protect themselves and others.

Films & Games: Understanding Age Ratings

It can be confusing to know what games or films are suitable for your child. The key is to understand the age ratings—they are there for a reason!

Age Ratings for Games (PEGI)

The **PEGI (Pan European Game Information)** rating is on all game packaging and digital store pages. It indicates the suitability of the content, *not* the difficulty of the game.

PEGI Rating	Suitable For	Key Content Descriptors (Icons on the box)
3	All ages	Very mild violence (comical/childlike)
7	7+	Non-realistic, very mild violence; potentially frightening sounds/scenes
12	12+	Non-realistic violence towards human-like characters; mild bad language; sexual innuendo

Social Media Age Limits:

Most social media platforms (like TikTok, Instagram, Snapchat, and Facebook) require users to be at least **13 years old** to create an account. Primary-aged children should **not** have accounts on these platforms.




The Power of a Strong Password

A strong password is your first and most important line of defence against online threats.

How to Choose a Strong Password (The NCSC 'Three Random Words' Rule):

The UK's National Cyber Security Centre (NCSC) recommends using **three random words** to create a strong, memorable password or *passphrase*.

1. **Choose Three Random Words:** The words should be completely unrelated and not easily associated with you (e.g., not the name of a pet or school).
 - *Example:* → **ZebraPencilTeacup**
2. **Add a Twist (Optional):** To make it even stronger, you can mix in capital letters, numbers, or symbols.
 - *Example:* → **ZebraPencil3Cup!**

 **Things to AVOID:** Using your name, birthday, 'password', '123456', or anything that can be easily found out from your social media.

Managing Screen Time: Finding a Healthy Balance

Setting boundaries for screen time is crucial for your child's sleep, education, and physical health.

Tips for Control and Consistency:

- **Create a Family Media Agreement:** Discuss and agree with your child *when, where, and for how long* devices can be used. Write it down and display it!
 - *Example Rules:* No screens during mealtimes. Max 1 hour on games per day.
- **Implement Screen-Free Times:**
 - **Charge devices outside the bedroom** overnight to protect sleep.
 - Designate a "**Digital Detox**" hour before bedtime.
- **Encourage Alternative Activities:** Actively promote and provide opportunities for fun, non-screen activities:
 - Outdoor play (park, garden, riding a bike)
 - Reading books (physical or e-books)
 - Creative play (Lego, drawing, crafts)
- **Use Parental Controls/Timers:** Many devices and apps have built-in controls that allow you to set time limits. Use a simple kitchen timer to signal when a session is ending.

