🌐 Online Safety and Digital Safeguarding at St Andrew's CofE Primary School

At St Andrew's we are committed to equipping our children with the essential skills to navigate the digital world safely, responsibly, and respectfully. Digital-Safety is a core part of our safeguarding duty and is taught regularly through our Computing and PSHE curriculum.

🤝 Our Partnership: Home and School

Keeping children safe online is a team effort. The most effective way to support your child is by **talking openly** about the online world—its benefits, risks, and how to stay safe.

1. The School Approach: The SMART Rules

We empower our pupils by teaching the internationally recognised **SMART Rules** to guide their behaviour and decision-making online:

Rule	**What it Means**
S - **Safe**	Keep **personal information private** (full name, address, school name, photos).
M - **Meet**	**Never agree to meet** someone you have only spoken to online. Always tell a trusted adult if asked.
A - **Accepting**	**Do not open messages or files** from people you don't know, as they may be hurtful or contain viruses.
R - **Reliable**	Not everything you read or see online is true. **Check the facts** with an adult.
T - **Tell**	Always **tell a trusted adult** (parent, carer, or teacher) if something online makes you feel **worried, uncomfortable, or sad**.

2. Safeguarding Risk Areas (The 4 Cs)

Our curriculum addresses the four key areas of online risk:

Risk Area	Focus for Pupils	Parent Action Points
Content	Seeing inappropriate or upsetting material.	**Set Parental Controls** on all devices and home Wi-Fi networks.
Contact	Being contacted by strangers or people pretending to be friends.	**Know Who They Talk To.** Ask who they play games with and if they message people they don't know.
Conduct	Behaving unkindly or inappropriately online (cyberbullying).	**Model Good Behaviour.** Encourage kindness and ensure your child is thinking before they post or send.
Commerce	Financial risks, advertising, or scams.	**Keep Payment Details Private.** Ensure your child knows they must never click on ads or make purchases without permission.

🤖 New Focus: AI and Online Safety

Artificial Intelligence (AI) tools, such as chatbots and image generators, are becoming part of everyday life. While they offer benefits for learning and creativity, they also introduce new risks that parents should be aware of.

What Parents Should Watch Out For:

- **Inaccurate or Inappropriate Content:** AI chatbots can provide false or inappropriate information and advice, sometimes promoting unhealthy or harmful behaviours.
    - **Action:** Teach your child to **always double-check** facts from a trusted source (like an approved educational website or a book).
- **The Problem of Deepfakes:** AI can be used to create highly realistic fake images, videos, or voices (known as deepfakes). These can be used for bullying, blackmail, or to impersonate someone your child knows.
    - **Action:** Emphasise the rule: **Not everything you see online is real.** Encourage healthy **scepticism** about what they view or receive.

- **Over-Reliance on Chatbots:** Children, especially those who are vulnerable, can treat AI chatbots as friends or trusted confidantes, leading to emotional reliance or preventing them from seeking help from a human adult.
    - **Action:** Regularly **discuss the difference** between human and AI relationships. Reassure your child that a parent or teacher is always the best person to go to for help or advice.
- **Privacy and Data:** Most AI tools are not designed for young children and can collect personal information and track interactions.
    - **Action: Check the age rating** and privacy policy of any AI tool or app before your child uses it. Limit the amount of personal information they are allowed to share with any chatbot or AI service.

🛑 What to Do If You Have a Concern

If your child is upset, worried, or if you encounter an online safety issue:

1. **Stop, Screenshot, and Tell:** Stop the activity, take a screenshot (if safe and possible), and tell a trusted adult immediately.
2. **Contact the School:** Report any issues that involve a member of the school community or affect your child's well-being in school to the **Designated Safeguarding Lead (DSL)**: **Rebecca Ireland-Curtis** via **head@st-andrews-pri.cambs.sch.uk**
3. **Report to Authorities:** For serious concerns about inappropriate online contact or content, you can make a report directly to the **CEOP Safety Centre (Child Exploitation and Online Protection)**:
    - Click to Report a Concern to CEOP
4. **Report Harmful Content:** Use this if you have found **illegal, hateful, or harmful content online** that you want to be taken down, such as: bullying, threats, or illegal images.

    - Click to Report Harmful Content
    - Click to report nude pictures and have them removed.

🔗 Useful Resources for Parents/Carers

We strongly recommend the following resources for up-to-date guides on popular apps, games, and devices, and how to set controls:

- **Thinkuknow:** Resources for parents and carers from the National Crime Agency (NCA-CEOP).
    - Visit the Thinkuknow Parents Site
- **Childnet International:** Guides and advice on how to keep your child safe online and talking about their digital life.
    - Visit Childnet's Parents and Carers Section
- **Internet Matters:** Provides expert guidance on a range of online safety issues and step-by-step guides for setting parental controls.
    - Visit Internet Matters