ST MICHAEL
Catholic Primary and Nursery

Computing Newsletter

TERM 2 • NOVEMBER–DECEMBER 2026

Keeping ourselves and each other safe online



Dear Parents and Carers,

Welcome to our Term 2 Computing newsletter! Our main focus is computer safety and keeping ourselves safe online. As the evenings become darker and Christmas approaches, this is a good time to review how children use games, apps and devices. Working together, we can help them enjoy technology with confidence, kindness and care.

Our online safety focus

We want children to recognise unsafe situations, protect personal information and know when to ask for help. Our Catholic values remind us to treat people with dignity online, just as we do face to face.

Six top tips to share with your child

1 Keep private information private. Do not share your address, school, phone number, passwords or live location in games, messages or public posts.

2 Pause before you click. Ask an adult before opening an unfamiliar link, downloading something or accepting an unexpected offer.

3 Online friends may be strangers. Someone's profile, photograph or claimed age may be false. Never arrange to meet an online contact without your parent or carer's involvement.

4 Be kind with every message. Do not join in hurtful chats or pass on embarrassing photographs. Ask permission before sharing someone's image.

5 Leave uncomfortable situations. Stop chatting or watching if something worries you. Tell a trusted adult, even if someone has asked you to keep it secret.

6 You can always ask for help. Telling an adult is the right thing to do, even if you clicked something by mistake or broke a family rule.

Try asking tonight: "What would you do if a game or message made you feel worried?"

Ten checks for parents and carers

Set aside a few minutes with your child to work through these checks. Explain what you are checking and why. Revisit settings regularly, after updates and whenever a new app, game or device is introduced.

1 Know what is installed. Look together at the apps, games, websites and accounts your child uses. Include consoles, tablets, smart TVs and any devices shared with siblings.

2 Check age suitability. Read game ratings and each service's current minimum-age requirements. Use the correct date of birth; a younger child should not use an adult's account.

3 Set controls at every level. Check your broadband, mobile network, device and individual apps. Home Wi-Fi filters may not protect a device using mobile data or another network.

4 Review privacy and permissions. Choose the most private suitable settings. Check who can see posts and profiles, and whether camera, microphone, contacts or location access is necessary.

5 Check chats and friend lists. Review who can message, call or invite your child to a group. Limit contact to people you have agreed on. Disable unnecessary voice chat and direct messaging.

6 Check videos and livestreams. Use age-appropriate child profiles and content controls. Review search settings and autoplay. Watch together to understand what your child is seeing.

7 Protect purchases. Require adult approval for downloads and spending. Check saved payment cards, subscriptions and in-game purchases, including offers of virtual currency.

8 Secure passwords and updates. Use unique, strong passwords and a password manager where helpful. Enable two-step verification where available, especially for parent email accounts. Install security updates.

9 Review routines and wellbeing. Agree device-free meals, regular breaks and a bedtime cut-off. Charge devices outside bedrooms overnight and notice whether online activity affects sleep or mood.

10 Practise reporting. Find the block and report buttons together. Agree at least two trusted adults your child can approach and reassure them that asking for help will be welcomed.

Gaming and group chats

Play a game together and explore its chat features. Talk about invitations to private conversations, requests to move to another app and "free" gifts that ask for account details. Check class or friendship chats for unkind comments and pressure to reply immediately. An online contact can seem friendly and still be unsafe.

Parental controls help reduce risk. They work best alongside supervision, conversation and trust.

Step-by-step controls: NSPCC parental controls guidance

Privacy checks: ICO Switched on to privacy checklist

Stay alert to scams and misleading content

Stop and check unexpected messages. Scams may look like parcel updates, competitions, shopping offers or requests from someone you know. Do not follow unexpected links; open the official app or website yourself.

Protect account access. Never share passwords or one-time verification codes. Check requests for money through a separate, trusted contact method, even if the message sounds urgent.

Use official downloads. Avoid unofficial game downloads, cheats and offers of free virtual currency. Ask an adult to check before installing anything.

Think carefully about AI. Pictures, voices and videos can be altered, and AI answers can be wrong. Check surprising claims with a trusted adult and reliable source. Do not put personal details or children's photographs into unfamiliar AI tools.

New technology for Christmas

If your child receives a connected device, set it up before they start using it. Install updates, create a suitable child account, check privacy and parental controls, restrict purchases and agree where and when it will be used. Include internet-connected toys and smart devices in your checks. Take time to explore together.

If something goes wrong

Stay calm and listen. Thank your child for telling you. Reassure them that they are not to blame for someone else's harmful behaviour. Avoid threatening to remove devices simply because they asked for help.

Stop contact and report. Help your child stop replying. Record usernames, dates and details; save ordinary bullying messages where appropriate, then block and report through the platform. Do not download, screenshot or forward sexual images of children.

Tell the school. Let the class teacher or a member of the safeguarding team know about online concerns affecting your child. Do not wait for a school response if a child is in immediate danger.

Where to get help

Immediate danger Call 999.

Online sexual abuse or grooming Report to the CEOP Safety Centre: ceop.police.uk/Safety-Centre.

Suspicious emails and texts Forward suspicious emails to report@phishing.gov.uk and suspicious texts to 7726. If you have lost money, contact your bank immediately and report to reportfraud.police.uk.

Our family challenge for Term 2

Make a family online safety agreement: what we use, who we speak to, what stays private and when we switch off. Let your child suggest a rule for adults too! Practise: "If anything worries me online, I will tell…" and name two trusted adults.

Parent advice and activities: CEOP Education

Cyber security tips: National Cyber Security Centre

Christmas device advice: Ofcom

Keep talking, keep checking and keep asking for help.