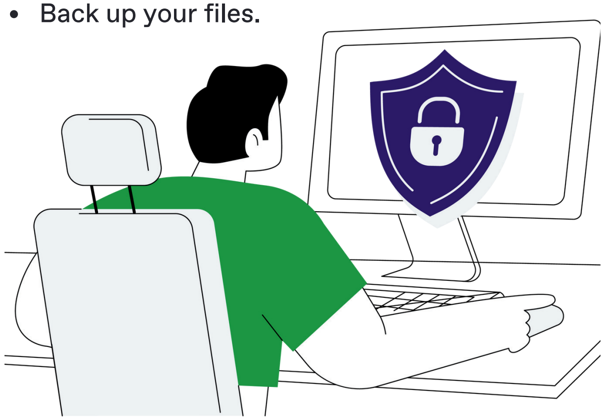
Devices & data

Your device is your gateway to the internet - keep it secure!

- Update regularly - install software and app updates to fix security flaws.
- Use antivirus software.
- Lock your screen - use a PIN, password or fingerprint.
- Only download from trusted sources.
- Back up your files.



Online gaming

Online games and communities can be fun and social, but they also come with risks. Be respectful in chats, avoid sharing personal information and watch out for scams or suspicious links. Use privacy settings and always report anything that makes you feel uncomfortable. Remember: block, report and tell an adult!

The future delivered. Seamlessly.

Cyberbullying

Cyberbullying is when someone uses technology to hurt, threaten or embarrass others. Don't reply or retaliate - block, report and tell a trusted adult. Save any evidence and speak up if you see it happening.

Being smart & kind online

When you're online, what you do matters. Here's how to use the internet safely and respectfully

- Be kind.
- Keep your information private – don't overshare personal information.
- Think before you post.
- Report harmful content.
- Be positive - help make the internet a better place.

My cybersafety checklist

□ I use strong passwords.

□ I know how to report online abuse.

□ I've checked my Privacy Settings.

□ I know who to talk to if something goes wrong.

Nortal | 25 years

Cyber security: Your digital superpower!

Helping students and parents stay safe online

nortal.com

Why it matters?

Every time you go online – whether you're gaming, chatting with friends, or handing in homework – you're sharing information. Some information is personal, such as your name, location or passwords. Cyber security is all about keeping that information (and your devices) safe from people who might try to steal or mess with it.

In today's digital world, online threats are real. Hackers, scammers, and viruses can target anyone – even students. But don't worry – learning a few simple cyber safety tips can help you stay in control and avoid becoming a victim of online crime.

Phishing

Phishing is when someone pretends to be a trusted person or company to trick you into giving away personal information.

How to spot a phishing message:

- It sounds super urgent or scary.
- The email or message comes from a weird or suspicious address.
- It tells you to click a link or download something.
- The link looks odd or has some spelling mistakes.

What to do:

- Don't click on links or download files from people you don't know.
- Check with a responsible adult.
- Report the message if you can.

Staying safe online

Top tips for staying safe online:

Use strong passwords – Make them long, unique, and hard to guess. No birthdays!

Turn on 2-Factor Authentication (2FA) – It adds an extra layer of protection.

Watch out for phishing - Don't click on weird links and always check who the message is really from.

Think before you share - Keep personal info like your address or school private.

Keep devices secure - regularly install updates and use antivirus.

What is 2FA?

What is Two-Factor Authentication (2FA)?
2FA is a free way to help keep your online accounts safe. It adds one more step when you log in - like getting a code on your phone, not just using a password.

Where can you use 2FA?
You can turn it on for apps like Instagram, Snapchat, TikTok, Gmail, YouTube, Xbox etc.

How to turn it on (example: Instagram):

1. Open the Instagram app.
2. Go to your profile and tap ≡ (top right).
3. Tap Account Centre > Password and Security > Two-Factor Authentication.
4. Choose how to get your code- by a text message or an authentication app.

What if anything goes wrong?

Even if you're careful, things can still go wrong. Knowing what to do can help you stay safe:

Don't panic - stay calm. Tell a trusted adult - like a parent, teacher or carer. Save any evidence - screenshots or messages. Change your passwords if you think you've been hacked. Block & report - don't engage with the person. Use official reporting tools. Learn & recover - it's okay to make mistakes!

For serious concerns (grooming, threats, exploitations), report to CEOP:
www.ceop.police.uk
NSPCC - 0808 800 5000
Childline - 0800 1111