The Safe Schools & Communities Team (SSCT) is a partnership between Dorset Police and the Dorset Combined Youth Offending Service, with a remit to prevent and reduce anti-social behaviour, crime and wrong-doing amongst children and young people, and help keep them safe in a digital world. The team consists of a number of Safe Schools Officers and a dedicated Internet Safety Officer located around the county.

Visit www.dorset.police.uk/ssct to find out more.

TOP TIPS FOR CYBER SAFETY

1. **Use strong, complex passwords.** Pets names, dates of birth and football teams don't make for good passwords. Use a combination of upper and lower case letters, numbers and special characters. A passphrase, made up of three random words, is a good base to start with.

2. **Install a reputable antivirus package.** Antivirus programs are a safety net, protecting you against any malicious files that find their way on to your devices. Make sure it's always on, and always up to date.

3. **Install updates.** Make sure you install software updates as soon possible. They often contain important security fixes

ONLINE SAFETY & CYBERCRIME PREVENTION RESOURCES

NSPCC ONLINE SAFETY WEBPAGE

Advice for parents and carers including parental controls, reviews of apps, conversation starters and contact information for the NSPCC/O_2 Parents Online Safety Phone Helpline. Parents can also book an appointment with an O_2 Guru.

O_2 NSPCC
Let's keep kids safe online

NSPCC

INTERNET MATTERS

Advice for parents of children of all ages – learn about it, talk about it, deal with it.

internet matters.org

COMMON SENSE MEDIA

Detailed reviews of games, websites and apps with the aim of helping parents make informed decisions about whether they are suitable for their children.

common sense media

ASKABOUTGAMES

Information about age ratings, tips about safe and beneficial play and discover the best games to play for different ages.

ask about games
From The VSC Rating Board

ACTION FRAUD

Action Fraud is the UK's national reporting centre for fraud and cyber crime. Report on the website, or by calling 0300 123 2040. The website also features warnings about emerging scams, helping to keep you one step ahead.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

4. **Be careful where you click.** Take care with links and attachments in email. If it's unexpected, or suspicious, don't click. Double check the address of the website the link takes you to (by hovering your mouse over the link). Criminals often take advantage of spelling mistakes to direct you to a malicious site.

5. **Beware of public Wi-Fi.** Whilst it's absolutely fine for casual browsing, free Wi-Fi is not secure. Sensitive data, like passwords or banking details, can be spied upon. Use your mobile data, or a Virtual Private Network (VPN) instead.

6. **Back it up.** Make a second or third copy of everything you care about. If you suffer from a ransomware attack, restoring files from a removable hard drive is much easier, cheaper, and more reliable than paying a criminal for your files back.

7. **Be careful what you share.** Where you go to school, or work, or on holiday… this information is more valuable than some people think. Information shared on social media can be used by scammers to impersonate potential victims, or guess password reset questions, for example.

8. **Keep your devices safe**. Use passwords, pin codes or biometrics where available.

9. **Use parental controls** on your broadband, devices and on accounts to control your childs privacy and security.

10. **Talk to your children** about safe behaviours online, and how to identify unsafe content, who they are talking to and what behavior they are experiencing. Children sometimes don't understand that people they speak to online are not friends, and could be hiding who they are. Support your children in using reporting and blocking tools and help them build their resilience.

11. **Use the recommended websites** to help you build your knowledge.

NATIONAL CYBER SECURITY CENTRE

The NCSC is part of GCHQ, the government's intelligence and security organisation. They provide impartial cyber security guidance for individuals and families, covering safe online shopping and gaming, strong passwords, protecting against malware, and other common cyber problems.

National Cyber Security Centre
a part of GCHQ

FINANCIAL CONDUCT AUTHORITY - SCAMSMART

There are scams out there for people of all ages, and the Financial Conduct Authority ScamSmart site provides useful information on financial fraud, including cryptocurrency, and other investment scams.

FCA FINANCIAL CONDUCT AUTHORITY

HAVEIBEENPWNED.COM

This site allows you to search across multiple data breaches to see if your personal details have been compromised. It can determine whether your email address and password are exposed online and provides guidance on how to secure your accounts if they are.

WWW.DORSET.POLICE.UK/CYBERCRIME

The Dorset Police Cyber Crime Unit's home page contains useful information, and links to resources to help keep you safe online. For further advice, our Cyber Protect Officer, Chris Conroy, can be emailed at cybercrimeprevention@dorset.pnn.police.uk.