GET SAFE ONLINE .org ®

www.getsafeonline.org

The young people in our families generally have a better hands-on knowledge of technology than we do. However, this confidence can result in them taking more risks onliine that could adversely affect their finances, reputation or even their whole future, if they end up with a criminal record.

If your young student is going to university or college this autumn, they may not have you there in person to guide them in the right direction or help if there's a problem.

#safestudentonline

That's why our experts have put together some tips to help you advise your child before they go. At the time this leaflet was written, we didn't know if universities would be open again. So whether your child is heading off shortly – or a little later – please take time to talk to them.

Safe banking

It's essential to follow their bank's security advice, including **keeping their banking and other financial details private,** and making money transfers safely via their bank's app. Suggest they get to know their Student Money Adviser.

Protect their reputation, and themselves

What goes online stays online, including things your child might regret sooner or later. Remember that 70%* of employers look at social media to screen candidates before hiring. Intimate images shared innocently can fall into the wrong hands. Location settings on phones and apps should be checked to help protect physical safety.

Identity and oversharing

Your child will need to prove their identity to open or access their bank account, sign up for a railcard, student discount or other essentials.

They should never reveal logins or other passwords and **not overshare** online, in texts or on the phone. This includes providing confidential information in return for freebies or to be entered into prize draws. Suggest they check their credit score regularly to make sure nobody has taken out credit or purchased anything in their (or your) name.

Mobile devices and Wi-Fi

Phones, tablets and laptops **should be treated like the precious possessions they are**. If what your child is doing is confidential or financial, they should avoid using Wi-Fi hotspots as there's no guarantee they're secure. Warn your child about location services on apps too.

** Figures taken from a 2017 survey from CareerBuilders: https://www.careerbuilder.com/advice/social-media-survey-2017*

Digital responsibility

Reinforce that there's **no place online for any kind of abuse**, hate speech, forcing their views on others or criminal activity.

Fraud

Fake texts, emails, DMs and calls claiming to be from the bank, student loan provider or HMRC are commonplace. Overseas students can also be targeted by visa fraudsters. Not thinking before they click – or oversharing – could cost your child their money, identity, or both.

Accommodation

If you child has found accommodation they like, help them **check it out in person and that the advertiser is authentic before any money changes hands.** Ideally, deposits and other up-front payments should be paid by credit card for extra protection.

Payments

Payment by bank transfer to an unknown person or company for accommodation deposits, fees or other costs or purchases should be avoided where possible. If it's a fraud, there's very little chance of getting a refund from the bank.

Online gambling

For some students away from home, **betting can become a bad habit**. Remind your child how much money and time they could be wasting and the positive things they could do with it. Point out the fine line between gaming and gambling.

Online dating

It's essential to use a reputable app and keep conversations on the app's messaging platform. Not everyone is who they claim to be … some even use online dating to commit fraud or endanger their date's physical safety when they meet up. **Tell them not to be afraid to block or say no.**

No means no

Your child should never be put under pressure to do something they feel uncomfortable with, or **put others under pressure**. This includes sending or publishing intimate pics, harmful pranking, extreme content, hacking others' social media accounts or any kind of radicalisation.

'Get rich quick' schemes

Students are favourite targets for illegal get rich quick schemes, like jobs with pay that's too good to be true or others using their bank accounts to 'process payments'. Money laundering could result a criminal record, even if it's done unwittingly.

Keep coding legal

Students who are **clever coders and extraordinary gamers** are sometimes targeted by cybercriminals who need their skills for malware coding or hacking. Talk to your child about the consequences, and discuss alternatives like a career in cybersecurity.

Find comprehensive, easy-to-follow advice about online safety at www.getsafeonline.org

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by a number of government departments, law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you have been a victim of fraud, report it to Action Fraud at actionfraud.police.uk or by calling 0300 123 2040. If you are in Scotland, contact Police Scotland on 101.

GET SAFE ONLINE .org

www.getsafeonline.org

OFFICIAL PARTNERS

TESCO · NatWest · Gumtree · Standard Life · first direct · PayPal · HSBC · Royal Bank of Scotland · M&S BANK · LLOYDS BANK · HALIFAX · BANK OF SCOTLAND · creativevirtual · ROYAL AIR FORCE · HM Government · CITY OF LONDON POLICE · NPCC · NATIONAL TRADING STANDARDS eCrime Team · cifas · VICTIM SUPPORT · EUROPOL EC3 · NCA · ActionFraud · METROPOLITAN POLICE · Ofcom · neighbourhood ALERT