Security

Think about

1. Passwords

Create a separate password for your email account. Make it strong with three random words using capital & lower letters, numbers & symbols. If safe to do so save the passwords in your browser.

2. Two factor authentication

Turn on two factor authentication where possible.

3. Your old accounts

If you've stopped using a social media site or forum there's no point in leaving personal information out there unnecessarily, deactivate the account and if you can, delete it.

4. Keep your anti-virus software up to date

Make sure you have anti-virus software installed on your device and be careful what you download or install on your computer.

5. Guard personal information

Unless necessary, restrict posting any personal information- your address, email address or mobile number - publicly online.

6. Back-ups

Turn on all back-ups.

7. In-App Purchases

Deactivate in-app purchases on your devices to prevent unexpected costs whist using apps and games.

ncsc.gov.uk/section/information-for/individuals-families

Information

Parents

- Talk to your child about what they are doing online
- Reassure them that they can talk to you if they are worried
- Use the tools that are available to manage their access
- Always check with your child about who they are chatting with and what types of conversations are taking place.
- It's always best to keep these video chats out in the open to avoid the dangers that can take place behind closed doors.
- Set up parental controls on their devices to control the level of security.
- Recognise that at the moment this is their main communication tool so they will be keen to get online and talk to their friends

.

Online Harms

In the first online safety laws of their kind, social media companies and tech firms will be legally required to protect their users and face tough penalties if they do not comply.

Ofcom will be the Regulator.

KEY TAKEAWAYS

- Independent regulator will be appointed to enforce stringent new standards.
- Social media firms must abide by mandatory "duty of care" to protect users and could face heavy fines if they fail to deliver.

ONLINE SAFETY

TIPS FOR YOUNG PEOPLE

Knaphill Federation of Schools

School Contact
office@knaphill.surrey.sch.uk

Resources and Assistance

Childline
0800 1111
www.childline.org.uk

Young Minds
0808 802 5544
www.youngminds.org.uk

NSPCC
0808 800 5000
www.nspcc.org.uk

CEOP
www.ceop.police.uk/safety-centre

The Parentzone
www.parentzone.co.uk

AACOSS
www.aacoss.org
enquiries@aacoss.org

TikTok

Hints and tips for TikTok

Set a Private Account:

1. Go to your profile page.
2. Tap three dots on the top right corner and select “Privacy and Settings”.
3. Select “Privacy and Safety” option and toggle “Private Account” on/off.

Enable Digital Wellbeing:

1. Select “Digital Wellbeing” under the app settings.
2. Tap “Turn On” and set a passcode.
3. Toggle “Screen Time Management” and Restricted Mode’ to turn these on.

Control Comments:

1. Go to App setting/Privacy and Safety settings.
2. Tap “Who Can Send Me comments”,
3. Choose ‘Friends or Off’ to limit comments to people your child knows on the app.
4. You can also turn off comments on individual videos by going to the menu button on the video and selecting ‘Comments off.

Manage Duet control:

1. In Privacy and Safety settings menu
2. Tap “Who Can Duet with me”,
3. Choose from ‘Everyone’, ‘Friends’ or ‘Off’.

Direct Messages

1. In Privacy and Safety settings menu
2. Tap ‘Who Can Send Messages to Me’
3. Choose from ‘Everyone’, ‘Friends’ or ‘Off’.

Block or Report

1. Go to the profile and click on the three dots at the top of the screen.
2. From the options select block a user.
3. To report a comment, tap the comment and tap report.
4. To report a video, go the video and tap the ‘share’ icon, tap report.

Houseparty

Hints and tips for Houseparty

Although the app is relatively secure as users can create “rooms” and pick only specific names of the people to talk with, if a child doesn’t “lock” their chat room and choose private settings, others can pop into the video chat.

1. House Rules – under the ‘House Rules’ section in the app, Houseparty has a list of “rules”. These are features that the app offers to help provide a better user experience and more security.
2. Room lock – users can lock the ‘room’ using a lock button on the bottom left side of the app’s home page. This prevents anyone from joining the room,
3. “Stranger Danger” – Houseparty advertises a feature called “Stranger Danger”, which alerts users when individuals they may not know, enter their room.
4. Location sharing – is an option to add other users who are nearby using a location-based “Near Me” option. This location-based searching can be turned off.

Fake News

Fake news is a type of false journalism or propaganda that consists of deliberate disinformation or hoaxes spread through traditional news media - both print and broadcast - or online social media

Instagram

Remember

1. You have to be 13 years of age to have an account.
2. Privacy settings allow you to determine who follows you.
3. Images are screen grabbed and re-circulated, so only post images you are happy to share.
4. Disable the feature where you share the location of where you took the picture.
5. Don’t accept friend requests from people you don’t know.

help.instagram.com

Snapchat

Remember

1. You have to be 13 years of age to have an account.
2. You can use a setting to only allow friends to send you ‘snaps’.
3. You can block a friend from sending pictures to you.
4. Snapchat can be set to let you know your message been opened.
5. It can be set to tell you that the recipient has captured and saved your picture.

www.snapchat.com/safety