Online Safety:

Information for Parents

Wednesday 1 December 2021

Private, rather than public, social media accounts are appropriate for those aged 13 years and over. Understanding the pitfalls around digital reputation is key. Searching for a young person's name regularly to check on their digital footprint will help them to maintain good habits. You should also check their browser history. By discussing the subject of digital wellbeing and agreeing daily limits before enforcing them, young people can enjoy their digital freedom healthily.

Passwords – 3 random words

Passwords play a significant part in cyber security and let's be honest, passwords are a pain.

Historically much of the advice and enforcement (particularly from tech companies and tech departments) has been around complexity, such as creating passwords that look something like " !aB6*lG16Bsthj ". This has never been good, pragmatic advice or enforcement for a number of different reasons, such as, "how am I going to remember that??".

A fundamental rule is this - a long password is a strong password. The longer the better. The National Cyber Security Centre (NCSC) has recently updated its guidance called '3 random words' and it is worth mentioning this to young people so they are able to create good digital 'habits' from an early age. Contained on the page is some clear, helpful advice as well as answers to some concerns.

You can read more on the NCSC website **HERE**.

5 terms every parent should know…

1. **Deepfakes** – Fake videos/images that allow people's faces or bodies to be swapped or digitally altered.
2. **Cancel culture** – the withdrawal of support for public figures or companies.
3. **Misinformation** – False information that has not been created to intentionally mislead people.
4. **Disinformation** – False information that has been created to mislead people.
5. **Digital activism** – using digital platforms to encourage social or political change.

Online Gaming & Fraud

Fraud, identity theft and general cyber security is something we need talk about a lot with young people. The reasons for this include: -

- Many safeguarding principles apply, e.g. private accounts, digital footprint.
- Older students take privacy of their data very seriously and want to know more.
- Many young people (and adults) don't understand how fraud can be carried out in games and social media, and so don't know what to look for.

Lloyds Bank recently carried out a survey and found that a fifth of gamers had either been a victim of a gaming-related scam or knew someone who had, but less than a third said they knew how to spot one. With fraud and personal identity theft being one of the biggest crimes around the world, that's a worrying statistic.

We often talk to young people about phishing and it is normally spoken about in relation to emails. Phishing scams are hugely popular in games and on social media, including YouTube, so it's important we are as up-to-date as possible in order to give students the right information. There is a short, recent article in the Guardian **HERE** which explains the rise in online gaming fraud..

Online Safety:
Information for Parents

If you are concerned about a young person at our school and you are unsure what to do, please email safeguarding@uptonhall.org. This address is only monitored during school hours. If you are concerned that a young person is in immediate danger, call the Integrated Front Door on 0151 606 2008/677 6557 or **in an emergency please dial 999.**

TikTok

TikTok allows users to create and share short, looping video clips which often involve lip-syncing or dancing to music and are enhanced through the use of filters and text.

Inappropriate Content – Whilst most clips may be seen as light hearted and amusing, some clips may feature drugs, alcohol, themes of suicide and self-harm and sexual provocation.

Explicit Songs – Some featured songs will contain explicit or suggestive lyrics. Some use racist or homophobic slurs.

Hazardous Visibility – TikTok is a really easy way to connect to others. Therefore, it is a platform for predators to contact teenagers.

Addictive – Social media platforms are designed to be addictive. Young people spend hours on such apps and this can negatively impact on sleep.

Advice for parents

Talk about online content – ask their opinion on what is appropriate and what isn't. Explain why they shouldn't give out their personal details.

Maintain privacy settings - Default settings for all U16 accounts are private. This will fortify their account against predators.

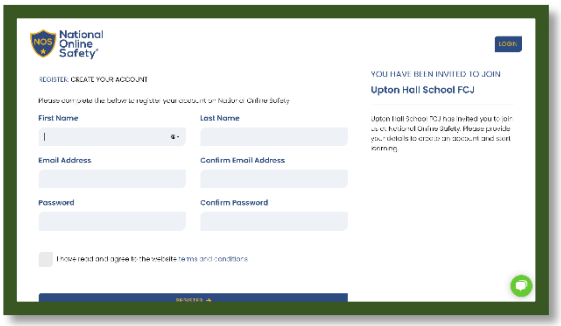
Block & report – Make sure that young people know how to block users and report inappropriate content.

Enable family pairing – Pair your own TikTok account with a young person so that you are able to control their settings from your phone.

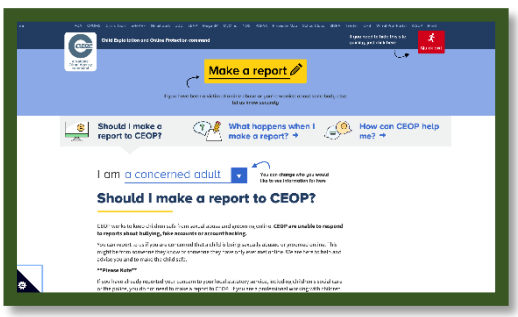
Restricted mode – filter inappropriate content that can be locked with a PIN.

Further Resources

As a National Online Safety accredited school, you can register for a free parent account where you will be able to access a plethora of resources that you can use to discuss online safety with young people. Visit https://nationalonlinesafety.com/enrol/upton-hall-school-fcj for more information.



You can also download the National Online Safety mobile phone app, available through both the App store and Google play. For more information, visit https://info.nationalonlinesafety.com/mobile-app.



If you think a young person is at risk, visit the CEOP website by clicking the link at the top of our home page. Young people and adults can use this facility.