At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

FaceApp, as the name suggests, is an app by Wireless Lab which uses uploaded images of someone's face and allows them to add a variety of interesting filters making themselves look older, younger, appear with different hair colour and so on. The app uses either the camera on your phone to take a selfie, or lets you use a picture from somewhere like Facebook or Instagram to apply these filters. While this all sounds like innocent fun, there have been some valid concerns raised about the terms and conditions, and what the company is doing with all these selfies and pictures.

AGE RESTRICTION

13+

If under 18, supervision of a parent or legal guardian required.

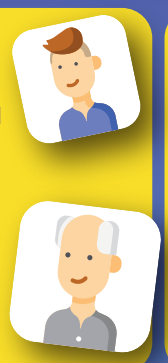
What parents need to know about FACEAPP

WHY IS IT SO POPULAR?

The app went viral in the middle of July 2019 with the #faceappchallenge, where users download Faceapp, take a picture of their face adding the old age filter, and then share the image of themselves online with friends. It can be fun to see what you might look like when you're more well travelled, and the results are pretty convincing (much to the amusement of older family members!).

HOW DOES IT WORK?

The app scans the uploaded face, and uses a neural network (basically a huge database of sample faces) to show what it thinks you'll look like when you're old; adding wrinkles, grey hairs, yellowed teeth etc. Anybody can upload an image they have access to, even those of children, without any kind of consent being needed. As explained in the lengthy terms and conditions of the app, these images are saved by Wireless Lab and can be used however they see fit, at any time in the future.



IS IT SAFE?

This is the contentious question. Wireless Lab, the Russian company behind the FaceApp app, are particularly vague with their descriptions of what they can potentially do with a person's details, to the point where a lot of people are worried about their images being used for nefarious purposes like cyber crime or political campaigns. In reality, the app is no more or less safe than any other, but that doesn't mean you shouldn't be vigilant of what you or your child is agreeing to online.

LEVEL OF ACCESS?

Buried in the legal jargon and technical mumbo jumbo, FaceApp has a worryingly large amount of access to your or your child's device. As well as storing any pictures you upload to the app, it also has access to your internet history, and basic information like your name and location. Naturally this sounds scary because it has been highlighted so publicly, but this is the normal kind of access and information apps take from us nowadays. If you are at all concerned it's worth leafing through those lengthy Terms Of Service before making a decision on if you're happy for your child to use an app.

SHOULD I BE WORRIED?

While your details COULD be used in the wrong way, the company has publicly stated they have no desire to do so and a number of independent probes into the app seem to suggest everything is being stored correctly and safely. That's not to say it will always be this way, so it's worth bearing in mind that this could change further down the line.

FACIAL RECOGNITION SOFTWARE

An app that takes an image of a face and uses it to commit online crimes or say things pretending to be somebody else might sound like the plot of a hollywood thriller, but with today's technology it can be a very real fear. Facial recognition software is now so advanced, a fake picture or video of a face can be produced without your knowledge or permission, potentially by a company you thought was safe. Now it must be stressed that this is extremely unlikely to happen, especially as this advanced technology is still being worked out, so you shouldn't be too worried about it - but always be aware of the permissions you're giving to unknown parties.

National Online Safety®

#WakeUpWednesday

Safety Tips For Parents

CHECK DOWNLOADS

It may seem obvious to keep an eye on what is downloaded on a device, but it can be very easy to miss out on new fads and viral hits. Most app stores let you see what's currently trending, alongside descriptions of what an app is. Talking to your child about what current trends they're enjoying will help you keep an eye on what's popular. You also get to see what you might look like in the future, which could be a blessing or a curse!

BE REALISTIC ABOUT YOUR DATA

When it comes to online security, the phrase 'better the devil you know' is particularly apt. While companies like Facebook and Google are by no means virtuous in their collection of our data, we do at least know (for the most part) a lot about how it's being handled. Luckily, we know Wireless Lab are treating our information correctly for now, but apps you don't know or trust, may not. It's always worth reading up on an app and making sure it's the real deal before downloading it.

BE AWARE OF COPYCAT APPS

When something like FaceApp goes viral, many copycat apps can pop up on the store piggybacking off the success of the original. These apps can contain viruses that are often far more malicious and dangerous to you and your child than the terms in the 'safe' version of the app. Make sure you're aware of which is the original before making any downloads.

KNOW IF YOU CAN SPEND MONEY ON AN APP

Like most things these days, there is a way to spend money on FaceApp. You can purchase a 'pro' version which unlocks additional filters either through your phone's app store, or on the app itself. This subscription ranges from 1 month for £3.99, 12 months for £19.99 or lifetime access for £38.49. It's very easy to make this purchase without too much thought so do make sure you know about any additional costs of an app your child is using.

ALWAYS READ THE TERMS AND CONDITIONS

Many of us don't have the time or energy to read through pages and pages of legal speak, and that's normal, but leafing through the fineprint can unearth a lot of grizzly permissions you didn't know you were giving. Often, at times they are unavoidable, but knowing what you're signing up for and if there's anything you can do about it could help you make more informed decisions on the types of content you expose your child to.

Meet our expert

Mark Foster has worked in the gaming industry for 5 years as a writer, editor and presenter. He is the current gaming editor of two of the biggest gaming news sites in the world, UNILAD Gaming and GAMINGbible. Starting gaming from a young age with his siblings, he has a passion for understanding how games and tech work, but more importantly, how to make them safe and fun.

SOURCES: https://www.techradar.com/uk/news/is-faceapp-safe-a-deeper-look-at-the-viral-hit, https://www.tomsguide.com/news/faceapp-photos-privacy-worries, https://fortune.com/2019/07/17/faceapp-safe-privacy-russian-old-face-app/ https://www.unilad.co.uk/technology/faceapp-could-be-sharing-all-your-photos-without-you-knowing/, https://www.faceapp.com/terms

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 23.07.2019

Bowood Halloween Adventures

Thursday 22nd October – Sunday 1st November

Pumpkin Trail | Falconry (25th, 28th October & 1st November)

Arts & Crafts | Autumn Walks

Family Days Out at Bowood House & Gardens

Adventure Playground | The Den & Activity Barn

Arboretum | Lake | Cascade | Caves

Bowood House | Walled Garden | Terrace Garden

Derry Hill, near Calne

Bowood.org