HATTON ACADEMIES TRUST

Gaming

Tips to stay safe

Set parental controls

Most games consoles have settings that prevent children from finding inappropriate games

Talk to your child and get involved

Take an active interest in the games they play and how they work. Better yet, have a go at playing it yourself

Use devices in a shared space

Monitor spending

Disable private messaging

It can increase risk of bullying, potential grooming and exploitation

Stay alert for scams

Agree digital boundaries

Agree how long they can play for and who they are allowed to play with

Encourage them to think critically

Remind them not to share personal information and not add any gaming friends to their social media networks

Online Safety Newsletter

Autumn 2022

FIFA 23

FIFA 23 will be the last in the well-known series, before EA launch their own football title next season. This 'end of an era' vibe has made it a must-have purchase for football-enthusiastic young gamers. The latest updates this year have focused on FIFA Ultimate Team mode, which can tempt gamers to spend real money recruiting better players for their side and this can put pressure on children to keep buying to compete with their friends. There are also other features in the game, which might pose some risks for children.

What are the risks?

In-game promotions

Children can spend significant sums attempting to improve their Ultimate Team. Some sought-after stars can be obtained more quickly with large amounts of FIFA points, which often cost real money.

Addictive nature

One match often leads to another, which could start affecting homework and bedtime. Children earning coins and swapping, selling and buying players can also be addictive and gambling-like.

Age-inappropriate chat

With many players enjoying audio chat through headsets, the mixed age range of players and a lack of regulation, chats can often turn offensive or toxic.

Circling scammers

Scammers can convince children to pay real money for fake FIFA points or player cards or can direct them to phishing sites that can access your payment information.

Social Media
Tips for your child to stay safe

Keep the computer in a shared area

Allow your child a limited set time each day

Request that you have access to your child's account credentials on social media

Use that to check for their activities, any suspicious friends or nasty messages

For older teens, require them adding you as a friend on social media

To monitor their activities via your own account

Enforce age requirements

Each app has its own minimum age but most of them require users to be at least 13

Review privacy settings on your child's profile

Teach your child about privacy

Posting content online gives the app the right to do whatever they wish with it including sharing it elsewhere.

BeReal.

BeReal is the latest trending social media app. The concept is that people see others in their authentic day-to-day lives, sharing candid photos without editing or applying filters. Each day at a random time, users are simultaneously notified to take a picture of what they're doing at that exact moment and to submit it in a two-minute window. BeReal shares 2 pictures: a selfie and an image of the immediate surroundings. Users can only view and react to their friends' photos once they've submitted their own.

BeReal.

BeReal's goal is for users to be authentic with friends, removing the pressure of flawless photos or perfect posts. It is still vital that children stop and think rather than uploading a risky picture to meet the 2-minute deadline. Remind them what strangers can extract from photos: school crest, street name, local landmark, etc.

Connecting with strangers

The 'Discovery' feed on BeReal shows posts from strangers and gives users the option to add them as friends. This means your child could potentially connect and communicate with a stranger.

Public sharing

The app allows posts to be shared publicly and to see public posts. There's currently no moderation on content being uploaded so young users can be exposed to content that is not suitable for their age.

Visible personal data

BeReal allows for a profile picture, full name, approximate location and a short bio on users' accounts. Make sure this does not include anything that can identify where they go to school or where they live.

Reputational damage

What your child does or says online – their digital footprint – shapes the way that other people see them.

Social Media Facts

Instagram
Minimum Age: 13 years
As long as the account is private, no one can view or comment on a post

WhatsApp
Minimum Age: 16 years
Limits access to people on your contact list but people in group chats not on your contact list can talk to you

Snapchat
Minimum Age: 13 years
Discover feature may allow children to access inappropriate content

Twitter
Minimum Age: 13 years
Even though Twitter has the option to delete a tweet, the posted content could have been copied or stored.

Facebook
Minimum Age: 13 years
Lets users share pictures, videos and comments

TikTok
Minimum Age: 13 years
TikTok defaults accounts to private and users must approve followers and comments. You can link your account to your child's to enable privacy settings.

Cyber Bullying

According to the latest research by anti-bullying charity Ditch the Label, 69% of young people under 20 have done something abusive to another person online, while 17% of young people have experienced cyber bullying. It's important to have regular conversations with your child about the online world to help you find out if they have ever experienced or witnessed online bullying themselves. This will also give you the opportunity to support them and reassure them.

Check these suggestions on UK Safer Internet Centre to help you start the conversation:
https://saferinternet.org.uk/guide-and-resource/have-a-conversation

Setting Up New Devices for Children

If you are planning on giving your child a new device for Christmas, do not neglect to set it up safely to ensure your child and the device stay safe.

BBC worked with Internet Matters and came up with a checklist to help you set up a new device for a child:
https://www.bbc.com/ownit/the-basics/correctly-set-up-childrens-devices

Password Safety

It is important to share with your children why online security is essential and what role a password plays in protecting their information and privacy. Teaching your child to always use a strong password that they don't use more than once and never share with anyone can be vital in building a habit that will help with their online safety now and later.

Many children struggle to think of a password that is strong enough to protect their accounts. DinoPass is a password generator tool for children that generate strong passwords that are easy to remember. Try it out and you will probably find that it is a useful tool for adults as well:
https://www.dinopass.com/