

Ref: NMT/EHWB

December 2017

Dear Parents and Carers

Social media apps and websites

As a school, we are aware of some of the social media apps that young people may use to connect with the people around them. We are also aware of the potential risks that come with such apps, particularly with regard to pupil safety and bullying.

We wrote to you in May to make you aware of the risks associated with some key social media apps and websites that young people often have access to at home. This letter is available [here](#) on our website for your reference. Please find some further new information outlined below to ensure we continue to work together to keep our children safe online.

What are the risks to young people on social media apps?

- Disclosure of private information
- Bullying
- Cyber-stalking
- Access to age-inappropriate content
- Online grooming
- Encountering comments that are violent, sexual or extremist in nature

It is important to maintain open dialogue with your child regarding their use of social media from the moment they have a mobile phone to ensure that they are aware of these risks and know how to use social media apps safely.

When checking your child's phone to ensure they are using it safely, it can seem a tad overwhelming. You may well be greeted with an array of apps that you do not recognise, and so it can be difficult to identify which are safe for use and which are not. It can also be difficult to broach the subject with your child effectively to ensure a productive outcome.

The social media apps and websites outlined below come with some risks. It is important to be aware of these risks. It is worth keeping an eye out for them and discussing the risks associated with them should your child be interested in them or have the apps downloaded on their phone.

Proud to be part of the Bohunt Education Trust



Musically.

Musically is an app that encourages its users to create their own music videos. It is marketed as a worldwide creative platform. It is aimed at teenagers, and encourages them to post either to their friends or publically so it is important to ensure the videos are not available publically. It also has links to explicit adult videos, despite the security settings in place. It is easy to come across an explicit video without intending to, due to the sharing nature of videos.



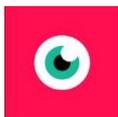
MeetMe.

MeetMe is an online chat room aimed at 13+ that randomly generates contacts for its user to talk to. It used to be called 'MyYearbook' and much of the communication is centred around meeting people online and meeting up. The purpose is to meet new people online as opposed to keeping up with friends.



Tinder.

Tinder is a dating app. Tinder's privacy policy allows children as young as 13 to register, as the app connects with Facebook. The geo-location features (where other users can see the location you are using the app from) and anonymous nature of this app puts children at high risk of connecting with people they do not know. This app is mostly used by adults and is not appropriate for children.



Live.ly.

Live.ly is an app that encourages its users to communicate with each other via live video link. There is therefore no security feature in place to protect what others post and what a user can therefore view, and often this can be inappropriate content, such as suggestive videos or self-harm videos.



Snapchat.

Snapchat is an app that allows users to send photos and messages to their contacts. These photos and messages can be viewed, and then disappear within 10 seconds of sending. Some users believe, wrongly, that these images disappear from devices once they have been sent. This is not true. Any

Proud to be part of the Bohunt Education Trust

user has the ability to 'screenshot' the image and save it to their device. These images can then be circulated like any other image.



Twitch.

Twitch encourages its users to video themselves gaming. There is also the function to chat with other users from around the world, therefore leaving users vulnerable to connecting with strangers on the app.



Vine.

Vine is Twitter's mobile app that allows users to shoot and share short loops of video. It is rated 17+, but anyone can download it. It is easy for any user to run a basic search and find offensive language, nudity, drug use and sexual videos. Whilst this is not the sole function of the app, it is there for all to view.



After school.

After school is an app aimed specifically at secondary school age children. It is an anonymous forum for posting innermost thoughts and feelings. Naturally, therefore, the content accessible on this app can be personal, inappropriate and upsetting for others. It can also be targeted to bully other users. It was closed down previously for its ineffective management of threatening and abusive language, and has been reinstated with some additional privacy settings; although the risks to children remain the same.



Instagram.

Possibly one of the most popular apps for teenagers, Instagram is a photo sharing site owned by Facebook. The app is rated 13+. It is possible to change privacy settings on this app to block contact from unknown users and also block sharing their location. Despite this, however, many users choose to keep their profile open for anyone to view and contact them.



Yellow.

Yellow is an app for young people and encourages them to connect with strangers. It has a reputation as a dating app for children.

Proud to be part of the Bohunt Education Trust

Facebook – online craze

In recent weeks there has been an online Facebook craze, which encourages children to intentionally go missing for 48 hours. The ‘game’ consists of obtaining points through how many times their name is mentioned on Facebook in the search for them during these 48 hours. Police have therefore put out a warning to all parents to keep an eye on their children’s Facebook activity.

Vault apps: apps that are designed to hide content

As if staying on top of all these apps is not hard enough work as a parent, there are some apps that are deliberately designed to ‘hide’ information, photos and communication on a phone or tablet. These apps are often discreet with their icon and look like any other app, such as a calculator, thus deceiving anyone except the phone user of its function: to hide inappropriate content. These vault apps can be used to hide communication, such as sexting.



Secret calculator (iOS).

This looks like a calculator app, but once the user enters a code it accesses the secret storage. There is also a ‘secret’ camera function.



Private Photo Vault (Android, iOS).

This app works in the same way as the secret calculator although is not as discreet with its icon. It also contains an unfiltered web browser that users can access, which overrides any safety browser you have in place on your child’s smartphone or tablet.



Best Secret Folder (iOS).

This app prides itself on being hard to notice as a secret folder.

What should I look out for with vault apps?

If your child has more than one calculator icon on their phone, this may suggest that one is a vault app. You will not be able to access what is in a vault app without the passcode set up by the user, as any photos, videos and messages will not appear anywhere else on the phone or tablet.

Proud to be part of the Bohunt Education Trust

How do I have these conversations?

It is easy to panic if you see an app on your child's phone that you did not know they had. It is even easier to wonder how to best support your child with making the best decisions without pushing them away.

It should always start with a conversation. You may find these tips useful:

- **Do not accuse your child** if they have an app you are worried about. Ask them what they use it for, and discuss the positives and negatives of using it. Try to keep them on your side and show understanding of their thoughts to download it in the first place.
- **Discuss the potential risks** with your child and go over some general rules about how to stay safe online.
- Go through the **security settings** together on each app so that you are comfortable with these.
- Discuss the **deletion of any apps** with your child if you decide this so that they understand the reasons.
- Go to Settings and turn **Location Services OFF**. This will ensure that your child cannot be identified by location when using their phone.
- Make a rule that your child should always ask for permission before **downloading** any apps – even the free ones. You can then go through the privacy settings together for apps that are appropriate for children, and can discuss those that are not.
- Advise your child not to share any **passwords** with anyone, except you.
- **Tell your child to let you know** if they notice anything online that makes them feel uncomfortable.
- **Remember that your child has not done this deliberately to upset you.** They can often follow what others are doing and can be unaware of the risks involved.

As a school we will continue to teach all students how to best stay safe online and make them aware of the risks associated with online behaviour. At home, you are in the best position to monitor your child's online activity and have these individual discussions with them to ensure they stay safe.

Remember that if you are ever concerned about something potentially harmful you find on your child's phone, and would like to seek advice, call the Police on 101 who will be able to assist you further.

Thank you for your continued support with educating our children on the risks of social media use and encouraging good habits and positive behaviours.

Yours faithfully

N Moffatt
Ms N Moffatt
Assistant Headteacher

Proud to be part of the Bohunt Education Trust