App Fact Sheet (updated September 2017)

Below is a brief outline of the most popular Apps students are using with a description of what they do, the risks and what parents/teachers should know about security options with them. It is not an exhaustive list nor does it cover everything about security. These are gathered from extensive visits to schools where the workshops identify current social media use or awareness trends among 4th-6thclass students. Parents should also be aware of the age and theme appropriates of the games their children are using and can learn more at **pegi.info**.

FaceBook

Age: 13+

Good to Know: Facebook allows users to put their location on every post and this is something children should not be doing. By default anyone on this app can send a child and friend request. This can be prevented by configuring security settlings (see below). Being a "friend" to your child does not mean you see everything they are doing as it is possible to select specific people/groups within a profile. There are a lot of third party apps (usually games) which can be downloaded within Facebook. In order to get these games children have to agree to the privacy policy which states what information the app will collect about the user. Remind children not to click "Allow" unless they/you are informed about what information they gather.

Risks: Like all online social media platforms the risk of Cyber bullying exists. Recently however this app is becoming less popular among teens as more instant forms of communication are favoured. Another potential issue here is that a child may connect with a friend of a friend who may be an entire stranger.

Security options: Under "*Privacy Settings & Tools"* there are 3 main headings which are 1) Who can see my stuff? 2) Who can contact me? 3) Who can look me up? These should be configured properly to ensure basic safety. There are further settings which limit the ability for others to post to a person's timeline and also influence whether a person can be tagged in a picture (i.e. their name identified on the photo. Please remember no matter how private an account is other users a person is connected to may not have the same level of privacy thereby anything shared to those people may be viewed by strangers.

Twitter

Age: 13+

Good to know: This is for the most part a public app which is very popular among teens to instantly share content between friends. It is also a way they can follow others such as celebrities and popular events both locally and globally. It's rapid and concise and this is what makes it attractive to many young people.

Risks: As this app is mainly public there is a lot of content on it (videos/pictures) which may be inappropriate for children. There are also a lot of ads that come up on it promoting various groups, companies etc. There is also the risk of Cyber bullying via "sub-tweeting" which is where tweets are circulated by a group about another person(s) without naming the individual(s), yet everyone knows who it is aimed at.

Security options: It's best not to use location sharing services as this can give away a child's location and could result in a face to face meeting!Tweets can be set to Private and this is something teens should be doing although it's not popular for them. You can also choose to block people who follow you. Within "*Privacy & Safety"*you can tick and un-tick boxes such as; who can tag me in photos, let others find me by email; let others find me by phone number etc.

Instagram

Age: 13+

Good to know: Used for sharing pictures and editing them in fun ways. People can comment on these and receive instant feedback on what they post. This app also enables sharing on other social media platforms and is extremely popular with teens at the moment. By default all of your posts are public and as you post a "Photo Map" can be created based upon the location of those pictures.

Risks: Comments about people's posts can become mean quiet quickly hence the risk of Cyber bullying. Also it is possible for young people to have followers who they don't know and this poses an obvious risk.

Security options: There are a number of security settings on this app including choosing it to be Private. This way only your followers get to see your posts and anyone else must request permission to do so. Another safety option is not to add your phone number when setting up the profile. Location can be turned off and this can help prevent strangers finding out about your whereabouts.

WhatsApp

Age:16+

Good to know: Allows the sharing of text and video content as well as making calls. This app is currently very popular for sending group messages

Risks: It can enable risky behaviour such as sexting and sharing other inappropriate content. Also the app doesn't require a password to be set to use it so if a child's phone is picked up by someone else many problems can ensue!

Security options: Control who sees your information by setting it to Everyone; My Contacts or Nobody. You can block specific contacts from interacting with you.

SnapChat

Age: 13+

Good to know: This app is currently the most popular amoung teens as it enables pictures to be sent to others and then set to delete after a short time. There is a version of it called “SnapKidz” for those under 13 which allows children to take snaps and modify them but not send them on. Video content can also be shared on it and

Risks: The fact that young people are attracted by the deleting aspect of the app they may be tricked or misguided into posting hurtful or inappropriate messages which could always be saved by others through a screeen shot.

Security options: The options here include: Who can Contact me; Who can View my story; Who can See Me in Quick Add. This should be set to Friends only where possible however it should be remembered that anyone you are in a group with will be able to chat to you in Group chat.

Viber

Age: 13+

Good to know: This app enables people to message, call and send pictures all over the world. Once this is installed it identifies through your phone contact list other users who have downloaded it. Popular with users is the sending of funny stickers in their messages, but this app also allows for large group chats and games to be played.

Risks: Group conversations can become hurtful quickly and on occasion young people can actively exclude others using it.

Security options: There are privacy settings which can give the user extra protection. You can set a block list and choose to hide online status. As a basic you can untick the box entitled “Share Online Status”. You can also select “nobody” as your profile picture status thereby minding your identity that bit more.

OOVOO

Age: 14+

Good to know: This app allows users to video chat with people online across phnoes, pcs, tablets etc. It allows those using apple devices to chat easily to those on andriod without any compatibility issues. Also it allows those using it to chat with up to 12 people at a time. While handy for study group meetings it can mean a lot of wasted time just “hanging out” online.

Risks: Children could be talking to anyone. There is also the risk of unsolicited inappropriate content popping up on screen.

Security options: Settings should be adjusted to Nobody meaning no one other than friends can follow them. There aren't many more strong options in it.

Musical.ly

Age: unclear

Good to know: This is a video based platform enabling users to make their own music videos and post to their friends. It also allows users to grow a fan base. All accounts are public by default so when users post there is no restriction to who can view it.

Risks: exposure to inappropriate and adult themed content is a big risk. Also the fact that it is public by default means anyone can follow another person unless it is configured to "private".

Security options:"Hide location info" and "Private account" are the two main settings within the security options.