POLICE
SCOTLAND

SOCIAL MEDIA INFORMATION

Below is some information relating to social media sites and applications for smart phones and tablets. It has been taken from open sources and is a generalisation of how they work, rather than a description of how individual apps operate, as popular apps can change month by month.

Most social media apps are free to download and allow users to find and share messages, chat, photos and videos on smart phones & tablets. They usually allow a user to browse a site without an account but individuals must have an account to use it. Most apps allow for a user to have multiple usernames.

Group facilities allow users to send messages and pictures to more than one user, by simply adding the user to a conversation. Once a user is added to a conversation, they will receive all messages sent as part of that conversation.

Some sites have a minimum user age of 13 years, although there is rarely an age verification system. In general, to register, the user must provide name, email address, phone number and password which must then be verified via email. Most apps display a username rather than mobile number or email address.

Many apps have a "Suggested Friends", "People You May Know" or a similar feature. When you sign up you are usually prompted to indicate whether you want to receive these messages. If you elect to receive them the app will access and upload the phone numbers and email addresses (but not usually names) from your mobile device address book before hashing the number/email address and uploading them to its servers. Any numbers/email addresses as registered on that app will be notified to you, and you will be notified to them. After this process is complete the app will delete your address book information from its databases but retain your phone number and email address in hashed format to provide the suggested friends feature.

By using the "Find more people" or similar function, you are consenting to the app again scanning your address book contacts for any updated information and the process continues as above. By indicating you want to receive "you may know" messages or using the "Find more people" you opt in to use the Suggested Friends Feature and consent to the app to use your contact information and address book information as described above.

For most instant messaging sites, any messages or pictures sent will be deleted after the message has been delivered to the recipient, although the app will retain the message sender and recipient data and associate it with the user name.

In general, the only way of saving an instant message or image is to take a screen shot or copy and paste the thread onto an email or word document. Do you know how to do this?

You can usually change your first name, last name, email address, and profile picture (but not username) once registered. You may request deletion of your Personal Information but the provider may be required to keep this information and not delete it (or to keep this information for a certain time). When information is deleted, it will be deleted from the active database, but may remain in the archives.

Each app has its own security settings and reporting tools, and some are better than others. Most have a blocking feature and built in reporting facility and some have a system of reporting immediate causes for concern.

Photo and video sharing apps usually allow private users to add hashtags to photos so that only the private user and their approved followers will be able to see that photo. Anyone can see a user profile if 'photos are private' is not activated. If activated, to view the photo, a user must send a follow request and be accepted as a contact.

The important thing to remember is that most apps are run in a similar manner. Some apps are UK based, others are based abroad. The laws governing app providers will depend on the country they are based in, therefore each app will have its own security and data retention systems based on the legal requirements of that country.

The CEOP website is run to gather and provide information to the public and Police in relation to online child protection issues.

In the UK, there are various pieces of legislation pertaining to the use of 'communications systems'. The following points describe the different types of use or message content covered by legislation. Some of this legislation comes under sexual offences rather than communications offences.

- Persistent use of a public electronic communications network.
- Sending a message that is false, grossly offensive, indecent, obcene or menacing for the purpose of causing annoyance, inconvenience or needless anxiety to another.
- Intentionally causing a child to view a sexual image for gratification or to cause distress.
- Being involved in a sexual written or verbal communication with a child.

THINGS TO THINK ABOUT

- **Parents** - sit down with your child and learn about the apps they use.
- Think about what time of night your child is online – the later it is, the more likely it is that adults rather than other children will be online.
- Does your wi-fi need to be on at night or can you disconnect it at bedtime?
- **Kids** - Think about the legality of the messages and photos you post, and who could view or copy them.
- Look at who is on your contact list. Do you know these people? Don't fall into the trap of trying to have more online friends than your peers.
- Remember that anything you do via 'live webcam' can be recorded by whoever is watching.
- Consider how your registration email address is used and how the apps use your contact information.