SCHOOLS ICT

The ins and outs of Facebook in a nutshell

E-Sussex, E-Safe

Safeguarding all children in East Sussex all the time

East Sussex County Council

Provided by **East Sussex County Council**

What IS Facebook?

Facebook is a world-wide system by which people can share words and images. In its simplest form, that's it!

It is a product that comes under the generic title of "Social Media", however, this aspect of Facebook is only the surface – the part users play with. It is, in fact, a multi-billion dollar company that uses the information users post in a variety of revenue generating ways.

It can also be used to form groups of people with like-minded interests. There are millions of users worldwide, over 13, 000 servers, and millions of groups.

Facebook offers its users access to the product free of charge, and also offers unlimited storage.

Who uses Facebook?

Although Facebook has a lower limit of 13 years of age, it is known that there are many underage users. Children know how to set up a Facebook account (or know a friend who does), and it is common to find users from the age of 7.

Unfortunately, Facebook do not screen their users in any way. There is a "***Terms of Use***", and a "***Privacy Notice***", but it is rare to find a Facebook user who has read either document. In any event, the Privacy Notice is over 28 pages long and not designed to be easily accessible. Multiple mouse-clicks are needed to navigate the whole document.

Sadly, some very unsavoury people use Facebook. These range from terrorists to paedophiles to identity thieves and fraudsters.

But it's easy to control my Privacy Settings, isn't it?

Yes and no. While you do have a lot of control over who sees what you post, you will find that you do not always have the choices you might wish to have. For example, sometimes the choice is "friends" or "Anyone". If you want the choice "no-one", then you may be disappointed.

Also, ultimately you do not control your privacy settings, Facebook do. They have been known to remove all privacy settings for periods of time, and when software upgrades are made, this may also affect your account.

Do Facebook actively monitor content?

Facebook do take action if users notify them of breaches of their Terms of Use. For example, if you found an image on Facebook that should not be there, you can report it and Facebook will then take

a decision on whether it breaches their community rules. If it does, the image will be removed and the person who posted it will be notified. They will not, however, be told who reported the image.

What's a "Profile"?

When you sign up for Facebook, you create a "Profile". This can be a minimal amount of information, but Facebook do encourage users to add a lot of detail. Email addresses, mobile phone numbers, images, the list can be quite detailed.

NB – Young people with autism may want to fill out the entire profile, and they may be uncomfortable about not filling in each field. They may also not like the idea of putting 123456789, in the mobile phone number box because that isn't their phone number! Young people with autism need enhanced support when using social media and chat rooms.

There is nothing to stop people creating a false profile. Paedophiles may create a profile in which they pretend to be a young person (of either gender), in order to join Facebook groups of other young people.

Similarly, there is nothing to stop a person creating multiple Facebook accounts. All that is needed is an email address, and they are easy to obtain, and to think up a user name.

Facebook do NOT perform any checks on their users.

So how do I know if the person who has sent me a "friend" request is real?

The short answer here is that unless you know that person in the physical world, you have no way of knowing if they are real or not. If someone you know in the physical world sends you a request, you would be well advised to phone them and ask them if they sent a request before accepting it.

Why do I need to do that?

Sometimes, accounts are hacked. This is easy if the person creating it has not bothered with a secure password, and/or if they have not changed that password for a long time. Hackers can take over someone's account and abuse it in a variety of ways.

There are usually tell-tale signs that indicate if a friends account has been hacked. These might include:-

- Inconsistencies in what they say.
- Asking for information they already have about you. (Your best friend already knows where you live and what your phone number is – why would they ask again?)

- Using language that is not like them.
- Asking you to do something that is out of character.

People do abuse Facebook and use it for purposes other than those for which it was created.

We all have to be on our guard – ALL the time when using connected technology.

What are common abuses on Facebook?

This is difficult to answer as new abuses are thought up all the time. The main ones, however are:-

Facebook Rape	Where an account is hacked and then operated in the originators name. Usually some very unpleasant comments are made with the intent of causing trouble, or harmed reputation for the original account holder.
Grooming	It is known that paedophiles create false profiles with the aim of contacting young children. Sometimes they will send friend requests to the person they want to contact, sometimes they will join a friends site and watch the activities of the group.
Identity thieves	There is money in information. Identity thieves will befriend people with the intent of discovering their name, date of birth, place of birth, town of residence, etc. This information can then be used to acquire duplicate documentation, open bank accounts, take out loans, etc.
Hate groups	Sadly we are seeing a rise of closed groups (membership by invitation only) whose purpose is to verbally attack an institution such as a school, or an individual. This breaches Facebook community rules, however Facebook do not act unless a complaint is made to them, and even then, they may take the view that what is being said comes under the right to freedom of speech. Regrettably, we know that young users sometimes set up closed groups like this to cyber-bully others.

Late in 2014, it became clear that terrorist groups were using social media to coordinate their activities. This has led to a debate on the extent to which providers of social media should monitor the traffic across their networks. This could easily impact on the right to privacy and the debate continues.

So, how do I use Facebook (and any social media) safely?

You need to be on your game at all times when using connected technology. While the vast majority of online transactions are trouble-free, abusers are getting cleverer.

1) Your awareness starts with the logon page. If you have typed www.facebook.com into your web browser, just check, ***before*** you log in, that your computer has taken you to that site. Sometimes malware can redirect you elsewhere, so check the address before you log in.

This is particularly important if you have used a punch-out button from another website. The familiar blue and white F  appears on many websites, but it doesn't always take you to Facebook. If you use one of these, always check it has taken you to the real Facebook login page, and not somewhere else.

2) Take a look at your page when it loads. Is there anything there in your name that you did NOT post?

3) Take a look at any friends requests. If they don't come from people you know and trust in the physical world, ignore them. You don't have to give a reason – just decline them.

4) Remember that invitations to join groups may make your information visible to people you do not know.

5) If someone Googled you, and saw your Facebook page (remember, sometimes privacy controls are turned off – you can *never* be sure your account is private) what does it say about you? Employers, colleges and Universities often Google applicants in order to see if what is on the application form matches the person they want to interview. Comments on social media may look funny at the time, but may come back to haunt you later. *(EG A student once put "Got so drunk on Sunday, couldn't be bothered to go to college till Wendesday!" on their site. This person was not getting any interviews despite having an excellent degree. Her whole Facebook site was a torrent of foul language and indicated a high degree of unreliability.)*

6) If you are in employment, your employer may have an interest in what you say in the public domain. There should be no comments about your work, your clients/service users, or anything that could bring your employer or their business into disrepute. We all have bad days – Facebook is NOT the place for airing grievances. Can employers discipline and even sack workers for this kind of thing? Yes!

7) Some groups of people need to operate social media with an enhanced level of discretion. Among this group are teachers, health care professionals, social workers, etc. Under **no** circumstances should clients or service users ever be on your friends lists, no matter how well-intentioned.

8) When using the product and responding to people you know, always be on the lookout for the strange comment that does not sound like them. Spellings, too, can be an indicator that their account may have been hacked. Remember, online, there is no need to reply to anything you find odd. You can just stop the conversation in its tracks until you have spoken to the person.

Finally, be particularly suspicious if you get a friend request from someone claiming their original account has been hacked so they've set up a new one. **ALWAYS** check this with them in person.

Sounds like its more complicated than I thought?

It is. You are using a global system with millions of users, some of whom are up to no good – you need your wits about you – as do young users.

Remember there are social media products aimed at children, but they carry exactly the same risks as Facebook does. There are users and abusers on all social media platforms.

We need to teach our children a new way of living in the connected world – while we don't want to make them overly suspicious of others, they need a new "highway code" to learn how to live, work and play in the online world.

Facebook IS complex. Its uses and abuses are complex, and abusers are changing their behaviours all the time.

If possible, try to attend a Facebook Awareness Training session. Your child's school has access to specialist trainers who can unpack Facebook for you, and show you how to use it safely and avoid the common pitfalls.