

## Staying Safe On-Line

A PCSHE session delivered by PC Michelle Avery, Neighbourhood Schools Officer

PC Avery visited our school to talk to parents and pupils about the possible dangers of using social networking sites, such as Facebook, and how to make themselves as safe as possible whilst using these sites.

She began her session by asking the pupils how many of them already use these type of sites. Most of them said they did use the sites, especially Facebook. She then asked them how many of them were aware of the 'panic button' facility which allows them to report any violations or abuse. Not many pupils were aware of it, which, as she told them, was one of the reasons she had come to speak to them.

PC Avery explained to the pupils that they always need to remember that Facebook is a business; they make their profit by selling on the information that members put on their profiles to companies who use that information to target sales. These companies will use Facebook information to send e-mails to people whose profiles suggest they may be interested in a particular product. For example, if a member writes that they are a fan of a particular band, or film, they may be targeted by companies selling DVD's. She reminded them that once they sign up to Facebook, they no longer own their page; Facebook owns all the information that they put on it, and can use it for their own purpose, so they need to be very careful what information they put on their page. She also reminded them that all information they put on their page is kept; even if they delete it from their profile, it will never completely disappear. It will still be in existence, and as it is owned by Facebook, it can still be used.

She next talked to them about knowing who could be visiting their Facebook page. She told them to make sure that they used their privacy or account settings to make sure that only their Facebook friends could view their page. She also told them to make sure that they only accepted people they knew personally as friends, and never to accept someone who claimed to be a friend of a friend, or a friend of a relative without being absolutely certain that they were genuine; people may not be who they say they are. She said that this is one of the main ways that predators will try to befriend young people. They may spend all day on the Internet looking for 'prey' and anyone who has not got their security settings set up properly may be a target. She advised pupils to check their security settings and their profile and photos weekly, to make sure they had not been changed or digitally enhanced. If they found anything had been changed, this was a sign that their profile had been hacked. They should report any suspicions by using the panic button, which reports the page to CEOP.

ClickCEOP is on Facebook, and can be downloaded by clicking on Account then applications. CEOP, the Child Exploitation and Online Protection Centre is a multi-agency service dedicated to tackling the exploitation of children, tracking and bringing offenders to account. CEOP can track the IP number of any message and trace the sender. Abuse and harassment are both arrestable offences, so all Facebook users must be careful what they post about other people!

To make themselves as safe as possible, PC Avery advised students not to put information that could identify where they live, or where they go to school, as this could allow predators to trace them and even to follow them, without their being aware of it. She suggested they do not put photos of themselves in their school uniform on their page, as this could allow predators to see where they got to school. She told them not to put photos of younger brothers or sisters on their page, as many predators are trying to obtain access to young children. She also told them not to put photos of themselves on holiday, in beachwear or skimpy clothes on their page for the same reasons. Her advice was not to put a photo of themselves on their page at all, but to put a picture of a dog or cat, or something similar on instead.

Her final points were tips for the students to bear in mind whilst using Facebook to avoid the possibility of problems arising. She told them always to be on high alert, as there are lots of people out there trying to hack into unsuspecting users accounts.

- The first tip was to always stay in the main chat-room, never taking up anyone's suggestion of moving to a private chat-room. Private chat-rooms cannot be monitored and cannot be reported for abuse.
- The second tip was to keep the home computer in a 'public' place, such as the living room or dining room. Abusers are unlikely to send any unpleasant messages if they think anyone else might see them. If students have their computer in their bedroom, they should not admit this to anyone in a chat-room. An abuser reading that message, will know that the computer is not being monitored, so they are more likely to send inappropriate messages.
- Thirdly, students need to be very careful about what information they give out about themselves. Even something as innocuous as telling someone they don't know about their favourite band, or favourite film, could lead to them being offered tickets to a concert by an abuser masquerading as a friend. Just giving small snippets of information to someone they don't know, could lead to a predator building up a profile of them. Questions such as What's your school like? Who do you go to school with? Which bus do you use? Could allow a predator to identify them and where they live.
- Lastly, she reminded them again remain on full alert always, never to accept people they didn't know personally as Facebook friends, to remember to check their profile and security settings regularly, and to always report any abuse to ClickCEOP.