Remember…

- You have no way of checking that the person is who they say they are.
- **Avoid answering any personal questions.**
- Check out your Facebook or other social networking sites. What information are you giving away there that someone might use.
- **You can keep yourself safe online by following the "Zip it, Block it, Flag it" steps.**
- No one should be asking to meet you and encouraging you not to tell your parents or carers. If they do, that alone is suspicious.
- **You will not be in trouble for reporting a suspicious conversation to the police. They would rather investigate and find it is harmless than let someone who is out to harm young people get away with it.**
- You are in a powerful position. You make the decisions as to what you say and do online. Make SMART choices.
- **If something has gone wrong, it is far better to tell someone early.**
- Any adult working in your school, as well as your parents and carers want to keep you safe and will help.
- **Together, we can make E-Sussex, E-Safe.**

Zip it, Block it, Flag it.

Zip It reminds you not to give out personal information over the internet, in chat rooms or by any other means. Personal information includes photographs of you, your name, address, telephone numbers, bank account details, or anything else that is personal to you. Make a list of the things you should not give out.

Block It reminds you that you have the ability to block users in chatrooms, or websites that upset you or that you do not like. Ask your parents or your teachers how to do this.

Flag it means, in short, tell someone. The reporting button is available and more and more websites are including it as standard. You can also download a version of Internet Explorer 8 with the zip it block it flag it buttons on. Flag it can also mean just talk to someone about it.

The more responsibility you take, the safer you are. Set yourself standards of behaviour that you expect from yourself and others and review them regularly.

You do not have to put up with abuse….

….EVER.

My own laptop, with webcam in my room!

(A guide for children and young people)

eastsussex.gov.uk

East Sussex County Council

Congratulations!
You have the power to go online whenever you like, visit whatever websites you like and, well, do whatever you want. (Probably…unless mum or dad have locked it down!)
But as spiderman says "With great power comes great responsibility" Or, to quote a line from Jurassic Park "Just because you could, doesn't mean you should"

Modern laptops or Netbooks are powerful personal computing solutions and many have built in webcams. Here is some advice to help you stay safe online.

Webcam
How do you know if your webcam is on or off? Most of them have a little light on them, but remember, sometimes the light can break but the webcam still work! Make sure you know when it is on or off. (Do not pin the webcam to the start menu) You should also check what it is showing, especially when you move away from the PC. Can your school uniform be shown, or other information that may give away where you go to school or where you live?

Webcam chat is very popular, but remember, even if you do not keep copies of your online chatting, other people might. Once you say something, or allow an image to be sent, it is out there forever and you lose any control over it.

Pop-ups
Sometimes, pop-ups can appear. You should begin by switching on your pop-up blocker. Even then, some may creep through. Avoid them! You cannot "Win a laptop" or indeed any competition that you have not entered. All of these are scams to get you to part with money or information. Don't fall for them, not matter how attractive they look.

Scam email.
Not that long ago, scam emails looked tatty or suspicious. Nowadays, they look really professional. No bank will ***ever*** ask you for your personal details to be verified. They will never send you an email asking you to do that and certainly will never threaten to suspend your account. Just delete them. If your Bank or Building Society do need information from you, they will write to you.

There are also emails around that tell you that you have won a foreign lottery or that you have been left money. Another type asks for your help in getting funds released for charity and offering you a percentage. Again, these are scams and should be deleted.

Chain emails
These usually contain some kind of data mining software and are usually sent by someone you know who has fallen for it.

Anti-virus, Firewall, anti-spyware and anti-malware
Yes, you need all four on your PC, and yes, you need them running constantly and yes, you need to enable automatic updates. Now and then you may be asked to turn your firewall off. In short, don't.

If you have a spam filter, please use it! It learns by being used and the more you dump in it the less junk mail you will get.

Internet chatrooms
Be careful what you say and to whom you say it. (And also *where* you say it. You do not need to chat in "private")

Your Social Networking site(s)
How well could someone know you from the information on the public page of your social networking sites? Some young people have only a minimal landing page, and everything about them is available only to friends. Watch out, though, because some of the applications in use, particularly on Facebook can make changes to your privacy settings. What was private once may not be now.

Usernames and passwords.
It is good to keep your social networking, email and logon details private. You should never give them to anyone else and certainly never send them over the internet. It is too easy for others to discover what they are. You should also try to have a "strong" passwords and change it regularly. A strong password will be a minimum of 8 characters in length, and it should have letters, numbers and punctuation characters in it.

You should also have at least one capital letter.