E-Safety

The purpose of this page is to raise awareness and understanding of E-Safety issues amongst students and ensure parents/carers have the relevant information available so they can support their child. It is important that students understand how to keep themselves safe online and that parents discuss this issue regularly with their children.

Good practices include, keeping your username and password safe and not sharing with others. Never give out personal information like your name, age, address and school. Stay in control of your online reputation. You must tell a trusted adult if someone or something has made you uncomfortable or worried whilst on the Internet.

If you have any further questions please contact: office@bullerswood.bromley.sch.uk

Please use the links below for the Parents Evening E-Safety slides:
E-Safety Presentation for Parents
E-Safety Presentation for Students

Other useful Guides for parents:

Child Exploitation And Online Protection Centre

The NCA's CEOP Command is here to help children and young people. They are here to help, if you are a young person and you or your friend have been forced or tricked into doing something online, or in the real world.

They also have advice and links to support for other online problems young people might face, such as cyberbullying and hacking. Visit their Safety Centre for advice and to report directly to CEOP, by clicking on the Click CEOP button.

Google Safety Centre

Yahoo Safety Centre

Think U Know

Safer Internet

Get Safe Online

Digital Parenting Magazine

Vodafone How To Guides

Parental Controls

The Parent Zone

www.childnet.com

www.kidsmart.org.uk

www.digizen.org

A parent's guide to Facebook

Safer surfing:

- We recommend that children are supervised while using the Internet.
- It is possible to buy software which will restrict access to 'harmful sites'. Most Internet Service Providers (ISPs) will also provide an element of 'filtering' to avoid unsuitable content; but you need to set it up.
- No system will remove all unsuitable material.
- It is important that your children know what to do if they come across any material that they feel uncomfortable with. REPORT IT.

Some search engines are set up specifically for children to use such as:

Personal Details:

- Students should not give out personal details about themselves or others. This includes: full name, address, 'phone numbers, email addresses etc.
- Students should never make arrangements to meet anyone over the net.
- Students should never give anyone else their password.
- People should not give out bank/card details unless they have checked that the site is trustworthy and that they have anti-spyware installed on the computer.

Webspace (free web areas such as MySpace):

- There are a large number of people offering free webspace at the moment. While this is great for developing creativity, it also has dangers.
- Free areas are easy to upload information to; and many target young people in their marketing.
- Free areas often invite others to view your areas/galleries etc. While it is good to share, people need to consider who may have access to these areas. Avoid giving out personal details about yourself or others.

(Examples of free webspace..... www.zorpia.com, www.bebo.com, www.myspace.com
There are areas on these sites and adverts which you may consider inappropriate.)

The four big internet providers in the UK are BT, Sky, TalkTalk and Virgin Media. They all provide their customers with free parental controls and can be activated at any time. They have useful videos to help you set the level of control that you feel is suitable for your child. And if you have children of different ages, you can even set up separate User Accounts for each one. The link you need to find your provider's parental control video is:
www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls

Chatrooms/Forums/MSN:

- These have many uses but also have many dangers. It is very hard to know whether the person is really as they say they are. Even if the name is someone you know, that doesn't necessarily mean that your friend is the person doing the typing!
- It is also not always clear who else is 'listening' in to your conversation.
- There are usually 'moderators' who you can contact if you are unhappy with anything in a forum or chatroom.
-

On-Line Games:

- This is a rapidly developing area and can have the same dangers as chat rooms. This is particularly true of role-play type games. In this case people are very unlikely to be who they say they are!
- There are usually moderators you can contact if you are unhappy with anything.
- Never give out personal details or arrange to meet someone.
- On-line games are not restricted to computers.

Emails:

- Avoid opening emails from unrecognised sources. Never open attachments without checking who they are from and whether they are likely to be safe.
- Emails may carry viruses.
- Most anti-virus programs will scan emails for spam (unsolicited, bulk mail); as well as viruses.
- Avoid using CC (Carbon Copy) or the 'To' box when sending to multiple addresses. Instead use BCC (Blind Carbon Copy). You can set up a group; put your own address in the 'To' box and the name of your group in the BCC box. This offers some protection in that people don't automatically see everyone else's email address.

Bullying:

- Unfortunately, bullies like new technology just the same as everyone else. Children need to be very careful about who they give mobile 'phone numbers to; what they upload (if anything); who they give email addresses to etc.
- Texting; using camera 'phones; setting up websites about people; MSN; and group emailing are all ways that are being used by some bullies.
- If it happens – tell someone immediately, save all evidence you can.

Passwords:

- Be imaginative with passwords. It is amazing how many are 'guessed'. ▪ Try to make sure passwords are at least 6 characters. (The longer the better.) ▪ Avoid using postcodes or family names / dates etc.
- Using unusual characters such as £$%&*^ makes fraud harder.
- Mixing capitals and lower case letters usually makes passwords more secure.
- Some people hold databases of the most common passwords!

- Never give out your PIN over the Internet.
- Most common password info: http://ask.yahoo.com/ask/20041022.html http://geodsoft.com/howto/password/common.htm

Veracity:

Pupils should always be encouraged to think critically about the information on the Internet and to consider how trustworthy it is. Anyone can set up a website! Here is a guide to critical thinking…

http://www.ithaca.edu/library/training/think.html#end