John Willmott School

Guide to E-Safety

Does your child:

- **Use a mobile phone?**
- **Play online games?**
- **Use the Internet?**
- **Use Youtube?**
- **Use MSN?**
- **Use a social networking site such as Facebook or Twitter?**

If the answer is yes, then read this guide to help protect your child in the virtual world

Dear parents,

Today at school we have been celebrating 'Safer Internet Day 2013.' (Tuesday 5th February) and the pupils have been taking part in a number of activities during form time, guidance and all the house assemblies during the course of the coming week. Please take your time to read this booklet, and discuss all the issues inside as it goes hand in hand with what they've learned today. Communication is the key to staying safe online.

The internet is such an integral part of children's lives these days. It opens up so many educational and social opportunities, giving them access to, quite literally, a world of information and experiences. Whether on a computer at school, a laptop at home, a games console or mobile phone, our pupils are increasingly accessing the internet whenever they can and wherever they are. As you would protect your child in the real world, you will want to make sure that they are safe whatever they are doing. If your child understands the risks and can make sensible and informed choices online, they can get the most from the internet and stay safe whilst doing so - particularly from those people who might seek them out to harm them. So, how can you protect your child online? The answer is simple. If you understand the internet and understand what the risks are, there are a number of things you can do that will make your child safer online. According to Ofcom, 7 out of 10 young people aged between 12 and 15 years old in the UK have a social network profile. A large percentage of these access these sites through their mobile phone rather than a computer. This has changed the way that children and young people communicate with their friends and family.

On the whole, our pupils have a very positive experience surfing the web or chatting with their online friends; however, as a parent or guardian there are some potential risks you should be aware of, such as cyberbullying, downloading and copyright issues, identity theft, excessive use of technology, inappropriate, illegal and harmful content and grooming. This booklet will hopefully help you prevent any issues, such as these, from arising, and how to deal with them if they do. I hope you enjoy reading this booklet and it informs you on many e-safety issues that you may or may not already know about.

Also within this booklet, we will be giving you information on a new reporting system within school, who to approach regarding any e-safety issues as well as information regarding the new e-safety policy within school.

Finally, as a school we have embarked on a new e-safety accreditation called the '360 degree safe mark.' We are the first Birmingham School to start this process, which will show our good practice when it comes to e-safety.

Regards,

Mr A Thomas,

E-Safety Ambassador & co-coordinator or E-Safety at John Willmott School

Encourage your children to report inappropriate behaviour

If your child is experiencing problems or is being cyberbullied encourage them to come to you for help. If they are uncomfortable speaking with you, tell them to speak with a trusted adult - an aunt, uncle, a teacher or older sibling - to lend an ear. Be sure your child knows how to report abuse or inappropriate behaviour to social networking sites. With Facebook, for example, they can report abuse by clicking the report link. Other social network sites also have reporting mechanisms. We have also set up a SHARP (School Help Advice Reporting Page) system within school. There will be more information about this further on in the booklet.

What to talk to your child about?

- Make sure your child knows how to change their privacy settings.
- Don't allow anyone to bully you online, encourage your child to speak to an adult or teacher.
- Not to spend too much time online, using a mobile phone, gaming console etc.

What can I do as a parent?

Good communication between a parent and child is critical: Check the privacy policy of your child's internet, mobile, social networking and games providers so that you understand what kind of information they collect and what they use it for. Encourage your child to only share their personal information with people or companies they know. Suggest that they use a nickname (not their real name) on websites, chat rooms and other online forums. Help them to set up strong passwords (a combination of letters, numbers and symbols) and explain why they shouldn't share them with anyone. Make sure they use a PIN lock on their mobile. Discuss the fact that not everyone on the internet is who they say they are. Explain how information they use to register for websites, competitions, downloads and other internet and mobile services could be used by the companies in question (e.g. to send marketing emails). Advise your child to get permission from friends and family before taking photos or videos of them and to check that they're happy for the images to be published - not everyone wants to be famous. Make sure you have up-to-date anti-virus and anti-spyware software on your child's computer and make the most of built-in tools like pop-up blockers and spam filters. Teach them the risks and dangers of sharing passwords, phone numbers, addresses and other personal information. Consider where you place your computer, keep an eye on what your child is looking at. Be sure you have computer security software with parental controls. Encourage your children not to spend too much time online, using a mobile phone, gaming console etc. Encourage other activities and sports. Ask about your child's online friends, encourage them to have their "real" friends as their friends on social networking sites. If your child has an online profile, ask if you or a close relative can be an online friend (to help and support them).

Parents A to Z guide to technology

Apps: An abbreviation for application. An app is a piece of software. It can run on your computer, or phone or other electronic device.

Blog:Short for web log, this is an online journal that users update.

Cyberbully:A cyberbully is like the traditional playground bully, but the harassment of his/her victims takes place online. Harassment can include teasing another person, posting rumours/lies about someone, or publishing unwanted pictures of the targeted person in public forums such as social networking profiles, message boards, chat rooms etc.

Facebook:A popular and rapidly growing social networking site based on circles of networks. A person selects a network, such as a school or geographic location, and can then make friends with others in that network. www.facebook.com

Flickr:Online photo management and sharing application. www.flickr.com

Friending:"Friending" describes the act of making friends online through sites such as Bebo, Myspace and Facebook.

InstantMessaging:Also known as AIM and IM'ing. Instant messaging is communicating using a program, such as AOL Instant Messenger, Facebook chat or MSN, which allows you to communicate via text in real time. It's like a phone conversation conducted with your fingertips. Some mobile phones also support instant messaging.

Podcast/vodcast: Downloadable items that can be listened to via your computer and/or portable music player. Podcasts usually contain only audio while a vodcast contains audio and video. An example of a popular vodcasting site is YouTube.

Profile: Sometimes referred to as a "page", a profile is a user-created web page that enables the user to enter information about him/herself that they want to share online.

Skype:A software application that allows users to make voice and video calls and chat over the internet. Calls to other users within the Skype service are free, while calls to both traditional landline telephones and mobile phones are chargeable. www.skype.com

Smartphone:A mobile phone that offers more advanced computing ability and connectivity, example a Blackberry or iPhone.

SocialNetwork:Internet social networks focus on building online communities with like-minded people. They allow people to communicate and share information on a wide scale, and to find others who share similar interests. People share information by creating a user profile and then updating their profiles with status alerts, pictures, and other items of interest to them, e.g. Facebook, Bebo and Myspace.

Spyware:A software downloaded onto a computer without the user's consent or knowledge that can monitor and track a user's behaviour. It can collect information about web sites visited, and interfere with computer activity by redirecting to other web sites, install other software, and slow connection speeds.

Installing and regularly running programs such as anti-spyware or anti-virus software can help direct and eliminate spyware on your computer.

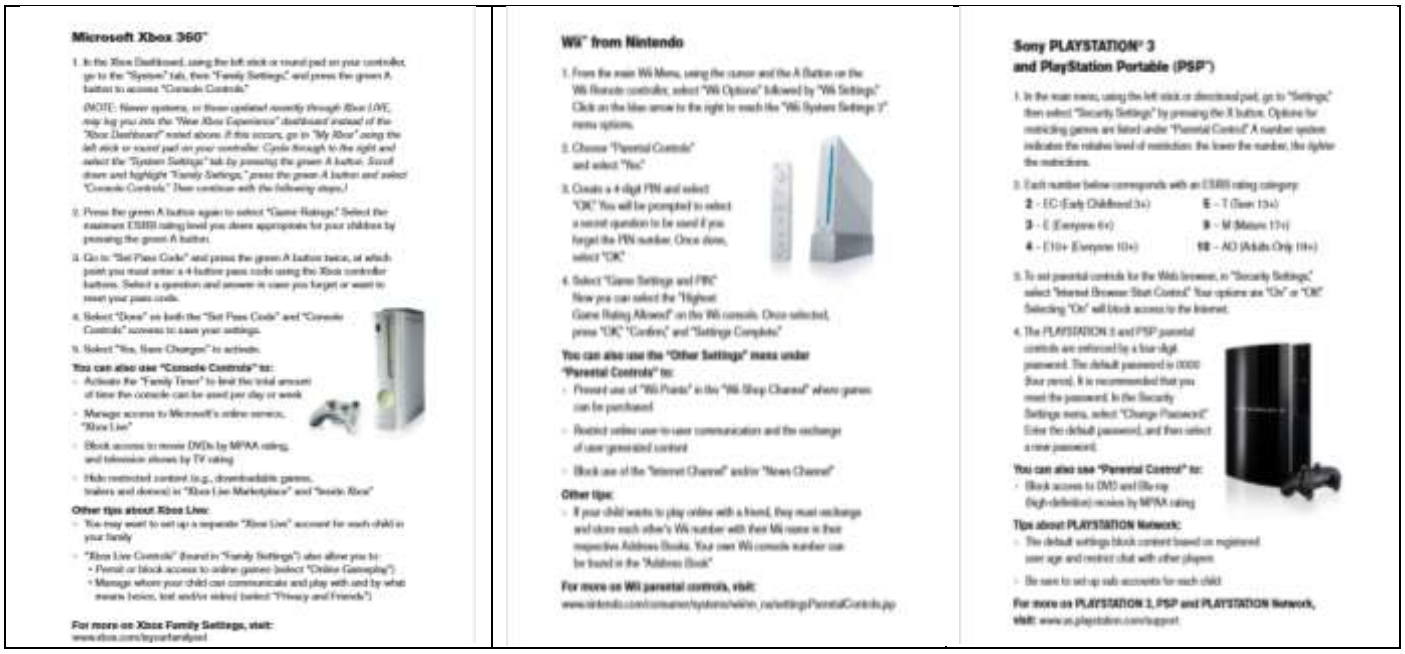
Tablet:A tablet PC is a wireless, portable personal computer with a touch screen. Usually a tablet is smaller than a notebook computer but larger than a smartphone, examples include the iPad.

Tagging:A label assigned to content on the internet in order to find it through searches more easily. Users on social networking sites such as Facebook can tag pictures with the name of the person in the picture so that others can find and view pictures of that person more easily.

Twitter:Sometimes also called a “tweet”. Tweets are live updates from a person sent via the web, SMS, or IM using the social network www.twitter.com allowing users to keep their friends posted on what they are doing at that moment. www.twitter.com

Wi-Fi:Short for “Wireless Fidelity”. A Wi-Fi enabled device such as a laptop or a mobile phone can easily connect to the internet when it detects that a wireless network is available. Wi-Fi hotspots make it convenient for owners of such devices to connect to the internet when away from home or work.

Video games – how to set parental controls



Microsoft Xbox 360™

1. In the Xbox Dashboard, using the left stick or round pad on your controller, go to the "System" tab, then "Family Settings," and press the green A button to access "Console Controls."

(NOTE: Newer systems, or those updated recently through Xbox LIVE, may log you into the "New Xbox Experience" dashboard instead of the "Xbox Dashboard" noted above. If this occurs, go to "My Xbox" using the left stick or round pad on your controller. Cycle through to the right and select the "System Settings" tab by pressing the green A button. Scroll down and highlight "Family Settings," press the green A button and select "Console Controls." Then continue with the following steps.)

2. Press the green A button again to select "Game Ratings." Select the maximum ESRB rating level you deem appropriate for your children by pressing the green A button.

3. Go to "Set Pass Code" and press the green A button twice, at which point you must enter a 4-button pass code using the Xbox controller buttons. Select a question and answer in case you forget or want to reset your pass code.

4. Select "Done" on both the "Set Pass Code" and "Console Controls" screens to save your settings.

5. Select "Yes, Save Changes" to activate.

You can also use "Console Controls" to:

- Activate the "Family Timer" to limit the total amount of time the console can be used per day or week
- Manage access to Microsoft's online service, "Xbox Live"
- Block access to movie DVDs by MPAA rating, and television shows by TV rating
- Hide restricted content (e.g., downloadable games, trailers and demos) in "Xbox Live Marketplace" and "Inside Xbox"

Other tips about Xbox Live:

- You may want to set up a separate "Xbox Live" account for each child in your family
- "Xbox Live Controls" (found in "Family Settings") also allow you to:
  - Permit or block access to online games (select "Online Gameplay")
  - Manage whom your child can communicate and play with and by what means (voice, text and/or video) (select "Privacy and Friends")

For more on Xbox Family Settings, visit:
www.xbox.com/en-US/familysettings

Wii™ from Nintendo

1. From the main Wii Menu, using the cursor and the A Button on the Wii Remote controller, select "Wii Options" followed by "Wii Settings." Click on the blue arrow to the right to reach the "Wii System Settings 3" menu options.

2. Choose "Parental Controls" and select "Yes."

3. Create a 4-digit PIN and select "OK." You will be prompted to select a secret question to be used if you forget the PIN number. Once done, select "OK."

4. Select "Game Settings and PIN." Now you can select the "Highest Game Rating Allowed" on the Wii console. Once selected, press "OK," "Confirm," and "Settings Complete."

You can also use the "Other Settings" menu under "Parental Controls" to:

- Prevent use of "Wii Points" in the "Wii Shop Channel" where games can be purchased
- Restrict online user-to-user communication and the exchange of user-generated content
- Block use of the "Internet Channel" and/or "News Channel"

Other tips:

- If your child wants to play online with a friend, they must exchange and store each other's Wii number with their Mii name in their respective Address Books. Your own Wii console number can be found in the "Address Book"

For more on Wii parental controls, visit:
www.nintendo.com/consumer/systems/wii/en_na/settingsParentalControls.jsp

Sony PLAYSTATION® 3 and PlayStation Portable (PSP®)

1. In the main menu, using the left stick or directional pad, go to "Settings," then select "Security Settings" by pressing the X button. Options for restricting games are listed under "Parental Control." A number system indicates the relative level of restriction: the lower the number, the tighter the restrictions.

2. Each number below corresponds with an ESRB rating category:

2 - EC (Early Childhood 3+)	**5** - T (Teen 13+)
3 - E (Everyone 6+)	**9** - M (Mature 17+)
4 - E10+ (Everyone 10+)	**10** - AO (Adults Only 18+)

3. To set parental controls for the Web browser, in "Security Settings," select "Internet Browser Start Control." Your options are "On" or "Off." Selecting "On" will block access to the Internet.

4. The PLAYSTATION 3 and PSP parental controls are enforced by a four-digit password. The default password is 0000 (four zeros). It is recommended that you reset the password. In the Security Settings menu, select "Change Password." Enter the default password, and then select a new password.

You can also use "Parental Control" to:

- Block access to DVD and Blu-ray (high-definition) movies by MPAA rating

Tips about PLAYSTATION Network:

- The default settings block content based on registered user age and restrict chat with other players
- Be sure to set up sub accounts for each child

For more on PLAYSTATION 3, PSP and PLAYSTATION Network, visit: www.us.playstation.com/support

Sharp system

There are many reasons why young people decide not to talk about incidents – confrontational, face to face, lack of confidence, scared, peer pressure, scared in case someone sees them talking to or seen in the schools office but to name just a few. As a result, we have set up a site that can help pupils report any issues.

The system is called **S.H.A.R.P** (School Help Advice Reporting Page).

The system can help us gather information as well as providing a lot of information for pupils regarding e-safety.

The link is found here…

http://johnwillmott.thesharpsystem.com/

On the webpage, pupils can anonymously make a report by clicking on the ‘make a report’ button on the bottom left hand side of the page. As well as this, they can look down the left hand side of the page.

PEGI AGE RATINGS AND DESCRIPTORS FOR VIDEO GAMES

Many of our children play video games, so it's important to understand the age ratings and descriptors provided on the back of all the video games that your children play.

	The content of games given this rating is considered suitable for all age groups. Some violence in a comical context (typically Bugs Bunny or Tom & Jerry cartoon-like forms of violence) is acceptable. The child should not be able to associate the character on the screen with real life characters, they should be totally fantasy. The game should not contain any sounds or pictures that are likely to scare or frighten young children. No bad language should be heard and there should be no scenes containing nudity or any scenes referring to sexual activity.
	Any game that would normally be rated at 3 but contains some possibly frightening scenes or sounds may be considered suitable in this category. Some scenes of partial nudity may be permitted but never in a sexual context.
	Video games that show violence of a slightly more graphic nature towards fantasy characters and/or non graphic violence towards human-looking characters or recognisable animals, as well as video games that show nudity of a slightly more graphic nature will fall into this category. Any bad language in the category must be mild and fall short of sexual expletives.
	This rating is applied once the depiction of violence (or sexual activity) reaches a stage that looks the same as would be expected in real life. More extreme language, the encouragement of the use of tobacco and drugs and the depiction of criminal activities can be included in this category.
	This adult rating is applied when the level of violence reaches a stage where it becomes gross violence and/or includes elements of specific types of violence. In general terms it is where the level of violence is so visually strong that it would make the reasonable viewer react with a sense of revulsion. This rating is also applied where the level of sexual activity is explicit which may mean that genitals are visible. Any game that glamorises the use of real life drugs will also probably fall into this category.

	The video game may refer to or depict the use of drugs.		The video game may be frightening or scary for young children.
	The video game may contain depictions of or material which may encourage discrimination.		The video game will contain bad language. At a 12 rating this will be mild swearing but at a 16 rating and above it will include sexual expletives.
	The video game may encourage or teach gambling.		The video game will contain depictions of violence
	The video game may show nudity in a sexual setting.		The video game may show sexual behaviour or sexual references
	The video game can be played online possibly with or against other people		

E-Safety policy

We have introduced a new E-Safety policy at John Willmott School, covering many of the issues below. A full copy is available on the school website, or if you would require a paper copy, please contact Mr A Thomas or Mr N Seabridge on the school phone number.

What our new E-Safety policy covers…

- THE IMPORTANCE OF INTERNET USE
- BENEFITS OF INTERNET USE IN EDUCATION
- USE OF THE INTERNET TO ENHANCE LEARNING
- PUPIL EVALUATION OF INTERNET AND ONLINE CONTENT
- MANAGING INFORMATION SYSTEMS
- INFORMATION SYSTEMS SECURITY AND MAINTENANCE
- EMAIL MANAGEMENT
- MANAGEMENT OF PUBLISHED CONTENT
- PUBLICATION OF PUPILS WORK OR IMAGES
- MANAGEMENT OF SOCIAL NETWORKING AND SOCIAL MEDIA
- INTERNET FILTERING
- MANAGEMENT OF VIDEOCONFERENCING
- EMERGING TECHNOLOGIES
- PROTECTION OF PERSONAL DATA
- INTERNET ACCESS AUTHORISATION
- ASSESSMENT OF RISKS
- SCHOOL RESPONSE TO INCIDENTS OF CONCERN
- E-SAFETY COMPLAINTS
- COMMUNITY INTERNET USE
- CYBER BULLYING
- USE OF THE VIRTUAL LEARNING ENVIRONMENT
- USE OF MOBILE PHONES AND PERSONAL DEVICES

Useful links for E-Safety issues

www.ceop.police.uk

www.childnet.com

http://www.saferinternet.org.uk/

http://www.iwf.org.uk/

http://johnwillmott.thesharpsystem.com/

http://www.swgfl.org.uk/

http://www.360safe.org.uk/7

http://www.thinkuknow.co.uk/

A parental ticklist for E-Safety

A how-to-guide to have good e-safety within your home

Computers, games consoles, mobile phones etc are the doorway to the online world. Think before you post online.	
Keep virus and firewall software up to-date	
Remember that passwords should be kept private and not shared with others	
Involve everyone and agree your family guidelines and rules	
Discuss that sometimes what is acceptable for a Year 11 child is not necessarily acceptable for a Year 7 child	
Regularly discuss online safety and go online with your children	
Talk together and have fun learning together	
Enable your 'browser safe' search option and/ or consider using internet filtering software, walled gardens and child-friendly search engines	
Critically view all content as some websites are not what they appear	
Keep the computer in a communal area of the house, where it's easier to monitor what your children are viewing	
Do not let children have webcams, or similar, in their bedroom. Remember any image, sound or text can be copied and viewed by everyone	
Talk to your children about why they should not to give out their personal details. If they want to subscribe to any online service then make up a family email address to receive the mail	
We all love to chat and children are no different. Encourage your children to use moderated chat rooms and never to meet up with an online 'friend' without first telling you	
Time spent online should be monitored to help prevent obsessive use of the internet. Children need to follow a range of activities many of which will be offline	
Encourage your children, and in fact all family members, to tell you if they feel uncomfortable, upset or threatened by anything they see online	
Have proportionate responses if the family guidelines are not followed	
What type of video games they should be playing	

Twitter page

John Willmott School are now on Twitter – please follow us for updates and important information.

https://twitter.com/JohnWillmottSch