SAINT JOHN'S

Family Guide to E-Safety

Dear Parents/Carers,

In this rapidly changing technological world it is important to stay up to date with all the latest developments and trends. Our children are growing up and embracing these new opportunities. Whilst these opportunities are hugely exciting, they also come with an element of risk. As you would protect your children in the real world, you will want to make sure that they are safe in the online digital world as well.

We hope you find this leaflet useful in supporting your children at home with e-safety.

Please share this with your child/children, especially the Be Smart poster included.

February 2018

WHAT YOU CAN DO RIGHT NOW

- Get inspired in your children's internet use. Discussing the opportunities and risks with children involves helping them to see for themselves how they might get into and out of danger
- Agree rules as a family about not disclosing personal information and check your children's privacy settings
- Bookmark your family's favourite websites and add www.ceop.police.co.uk to your favourites if you ever need to report online abuse to the police
- Encourage children to talk to someone they trust if they are worried or upset by something that happens online
- Make use of available filtering and monitoring software. These can help to block inappropriate material but remember they are not 100% effective
- Make sure your children know the SMART rules on (see attachment). These have been written especially for young people by Childnet
- 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.

AN A – 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 cyber bully 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.

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

Hotspots: A term used to describe locations where there is a Wi-Fi or wireless connection available. People can connect to the internet from their wireless internet devices such as: laptops, personal digital assistant (PDAs) and mobile phones, from this area.

Instant Messaging: Also known as AIM and IM'ing. Instant messaging is communicating using a program, such as AOL Instant Messenger™ 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.

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

Social Network: 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, Snapchat and Instagram.

Spyware: 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 detect and eliminate spyware on your computer.

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 allowing users to keep their friends posted on what they are doing at that moment. www.twitter.com. You can follow St John's on Twitter!

Virus: A computer virus is malevolent software designed to copy itself and spread to other computers without the user's knowledge.

Wiki: A website where users can add, remove, and edit pages using a web browser, e.g. Wikipedia the online free encyclopaedia. www.wikipedia.com

A GUIDE TO SAFE SOCIAL NETWORKING

* Do not let peer pressure or what other people are doing on these sites convince you to do something you are not comfortable with.

* Be wary of publishing any identifying information about yourself – either in your profile or in your posts – such as phone numbers, pictures of your home, workplace or school, your address or birthday.

* Use strong passwords and keep your profile closed and allow only your friends to view your profile.

* What goes online stays online. Do not say anything or publish pictures that might later cause you or someone else embarrassment.

* Never post comments that are abusive or may cause offence to either individuals or groups of society.

* Be aware of what friends post about you, or reply to your posts, particularly about your personal details and activities.

* Learn how to use the site properly. Use the privacy features to restrict strangers' access to your profile. Be guarded about who you let join your network.

* Be on your guard against phishing scams, including fake friend requests and posts from individuals or companies inviting you to visit other pages or sites.

* If you do get caught up in a scam, make sure you remove any corresponding likes and app permissions from your account. * Ensure you have effective and updated antivirus/antispyware software and firewall running before you go online.

Further Information

www.ceop.police.uk

The Child Exploitation and Online Protection (CEOP) Centre's website houses a range of information on how to stay safe online. It includes a unique facility that enables parents and young people to make reports of actual or attempted abuse online.

www.digizen.org

Provides information about using social network and social media sites creatively and safely

www.childnet.com

The Childnet International website gives internet safety advice and links for young people, parents, teachers and other organisations.

See our school's website for more information on keeping your child safe online or please speak to a member of staff.
www.st-johns-pri.gloucs.sch.uk

Encourage your children to visit the Kidszone section of the school website (under the Learning tab) for more information/activities on e-safety

Be smart on the internet

Childnet International
www.childnet.com

S SAFE

Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEETING

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ACCEPTING

Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE

Information you find on the internet may not be true, or someone online may be lying about who they are.

T TELL

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

THINK U KNOW

www.kidsmart.org.uk

KidSMART

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.