Keeping Safe Online

A Guide for Children

1. Never tell anyone online where you live, what school you go to, your address, email or phone number and never send pictures of yourself to anyone. If anyone asks you for this information you should tell your parent or carer.
2. Making friends online is great but NEVER agree to meet up with someone you have chatted to online. Online friends are still strangers and not everyone is who they say they are. If you do meet up make sure your mum or dad knows about it AND they, or another safe adult, come with you.
3. Never open emails, messages or files from anyone you don't know. They may contain viruses or nasty messages.
4. The internet is great for finding things out but not everything you read will be true. Check out what you read by looking at different websites, checking in books or asking your teacher or someone who knows.
5. Not everyone online is truthful about who they are and what they are doing. Sometimes people use the internet to bully, upset or hurt people. It is always safest to chat only to people online that you know in real life and make sure your parents know what chat rooms you use. If someone makes you feel uncomfortable, asks you to do something that you are not happy about or bullies you online, tell your mum or dad.
6. If you are worried about something you have seen online or something someone has said to you online, you can report it to CEOP (Child Exploitation and Online Protection) www.thinkuknow.net.

Keeping Safe Online - A Guide for Older Children

1. Always check that your parent/carer is happy for you to enter a chat room and try to make sure you only use chat rooms that are regulated and run by reputable organisations that monitor activity.
2. When you visit a chat room use a nickname and never give any identifying information such as your real name, age, address, email address, telephone number, school or church/youth group name. Remember chat rooms are 'public places' and you never know who might be in there and see it.
3. Keep your passwords private, don't even tell your friends.
4. Only give out as much information as you are happy with. If a site has a compulsory field you have to fill in and you don't think it is necessary leave.
5. Chat safely – you can't always be sure that it is only people your age in a chat room – it may be an adult winding you up or trying to trick you. Block people who make you feel uncomfortable and stay out of 'over-18' chat rooms, websites and other parts of the internet intended for adults. The warnings are for your protection. Adult sites can cost a lot more on your phone bill too.
6. Leave a chat room the moment anything worries you. Let your parent/carer/youth leader know and report any bad taste / bad attitude messages to the chat service provider / internet service provider. Save any conversations that you think could prove someone has been bullying or harassing you. If you are worried about something you have seen online or something someone has said to you online, you can report it to CEOP (Child Exploitation and Online Protection) www.thinkuknow.net.

7. Don't send via text or email your photo to anyone and especially do not send sexually explicit or revealing photographs of yourself. You may trust the person you have sent them to at the moment but sometimes people use such photographs to bully others when they are no longer friends. Don't think this cannot happen to you.
8. People you contact online are not always who they seem, and people don't always tell the truth online – no-one can see them. Never arrange to meet anyone without first agreeing it with your parent/carer and get them to come with you to the first meeting, which should always be in a public place.
9. Be careful when entering competitions etc. You may be signing up to services you don't want and never give out credit card or bank details without first checking with your parent/carer. If you pay for something online, make sure there is a credit card safety symbol on the site, it looks like a yellow padlock and means your details will be safe.
10. Never respond to nasty, suggestive, or offensive emails or postings in user net groups and do not 'Troll' (post inflammatory messages to wind people up).

Emails

1. If you get an email from someone you don't know, don't open their links or attachments. They could contain viruses which can damage or destroy your computer or lead to inappropriate or illegal sites.
2. Make sure your computer has virus protection software installed.
3. Never send chain letters via the internet – they are forbidden on the internet. If you receive one notify your Internet Service Provider.
4. Online fraud and scams are common. Be suspicious if you receive an email telling you that you have won a competition or lottery you haven't entered, or you get an offer that seems too good to be true. It is unlikely to be true!

Church's Acceptable Use of ICT Policy

If using church equipment, you must abide by the church's acceptable use of ICT policy. This means you must not:

1. Search for and/or enter pornographic, racist or hate motivated sites.
2. Use ICT provided by the church to store, display and/or transmit pornographic, sexist, racist, homophobic, or violent material.
3. Send emails or post messages or pictures on any social media site or otherwise use ICT in such a way as to threaten, intimidate, bully, or abuse any individual or group.
4. Download, forward and/or burn on to any CD/DVD any music, images, or movies from the internet without permission of the copyright holder.
5. Disclose of any personal information relating to others without their consent e.g., addresses (personal, email or messenger), photographs, telephone numbers or bank details.