SPRATTON HALL

Internet Safety Guidance for Parents

E-Safety @ Home

E-Safety is a key component in the ICT curriculum at Spratton Hall and pupils regularly complete activities designed to arm them with strategies to help them deal with a variety of situations they could encounter online.

Our philosophy is that ensuring each child is confident in these simple strategies is more effective than any piece of software would be in keeping them safe.

The strategies presented are based on recent research and advice as well as my own professional experience and knowledge. It is important to remember that we are not only talking about your computer when we talk about E-safety but also games consoles, digital television and particularly mobile phones which have become sufficiently sophisticated and accessible to children as to allow complete internet access in a very mobile form.

As parents, how many of the strategies presented in this document you will adopt and how you monitor your child's online activities is ultimately up to you. Please feel free to alter the Home E-Safety Agreement to suit your own personal preferences but remember that I have written it as it would be in place in my own home in order to ensure it represents the best possible practice for keeping children safe online.

E-Safety Agreement

This is a simple home agreement which can be used to help apply and consolidate these strategies as well as the rules you set at home for internet use. This should be displayed by the computer, signed by all relevant adults and children in the house that use it.

1. I will not give out personal information such as my photo, address, telephone number, or the name and location of my school. I will tell my parents if someone asks me for them.

2. I will use a nick-name online rather than my real name. I will give my parents a list of my friends who know these nick-names.

3. I will tell my parents right away if I come across any information, pictures or people that make me feel uncomfortable when I am online.

4. I will never agree to get together with someone I “meet” online without permission from my parents.

5. I will only use the internet at the times I have agreed with my parents and I will let them know what I intend to do online.

6. I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away.

7. I will only access areas of the internet which I have agreed with my parents. If I want to add a new site I will show it to my parents and explain why I want to use it.

8. I will not give out my Internet / email password to anyone (even my best friends) other than my parents.

9. I will be a good online citizen and not do anything that hurts other people or is against the law.

10. I understand that my parents need to have access to my passwords and my email / internet history. The more I show that I can be trusted, the more responsibility I will be given.

Strategies for Children

At Spratton Hall, every child from Year 3 upwards has specific E-Safety lessons built into the ICT curriculum each year. The aim of these lessons is to arm the children with a set of simple strategies to keep them safe online. These include:

- Never opening messages from or engaging in conversation with someone you do not know online.
- Never giving out personal information about yourself, your family or your friends.
- If someone you have “met” online asks you to meet them in real life speak to your parents immediately. You must never agree to meet someone you have met online without your parents’ permission. If they agree then one or both of your parents should go with you.
- Should you encounter something or someone that makes you feel frightened or worried online, tell a trusted adult immediately and show it to them.
- Never feel guilty about these incidents; they are not your fault.
- Remember that not all of the information you find online is true.
- Be careful what you download. Can you be sure of what you will get?

The SMART Approach (from Childnet.org)

SAFE – Keep safe by being careful not to give out personal information – such as your name, email, phone number, home address, or school name – to people who you don’t trust online.

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.

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!

RELIABLE – Someone online may be lying about who they are, and information you find on the internet may not be reliable.

TELL – Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried. You can report online abuse to the police at: http://www.thinkuknow.co.uk/.

Strategies for Parents

Setting Parental Controls

Your computer will have a range of simple tools to help you establish what your child can and cannot do on your home computer. Although it is impossible to cover every possible operating system or piece of software, the following pages will help you to access the most commonly available tools. Click on the links below to access advice on how to use these tools.

Parental Controls

These are the first thing you could do when you buy a new computer and yet very few of us have ever accessed them. Please remember that it is also worth setting the parental controls for your Sky TV box (or equivalent) or mobile phones in order to avoid the children accessing unsuitable content.

Parental Controls in Windows Vista

Parental Controls in Windows XP

Internet Explorer

The content advisor allows you to specify what your children should and should not be able to access. You can vary this as children grow. Individual sites which cause you concern can be blocked very quickly.

Content Advisor in Internet Explorer

Search Engines

A lot of the questions received from parents relate to their children using Google to search for information. This is, without question, the best search information on the internet. It is important to remember that the first and best line of defence is to supervise use of these search engines and ensure that children are not using rude words or searching for unsuitable content on purpose. By clicking in the drop down arrow at the end of the search bar you can check the recent searches which have been made.

It is also very simple to increase how strict the filtering of material is within Google. On the Google website, simply click on the Preferences link and then on SafeSearch Filtering.

There are of course other search engines to use and many of them are more child friendly. Here are a few examples:

- Ask Jeeves for kids
- Yahoo! Kids
- CBBC Search
- Kidsclick
- Zoo Search

Social Networking

Social networking sites such as Twitter, Facebook, My Space and Instagram are a means of communicating, sharing pictures, keeping people up to date with achievements or special events and playing games with friends no matter where they are.

Most of these sites have a legal age limit in place. The most common restrictions are that no child under the age of 13 may open an account and if they are under 18 they must be in full time education.

The dangers are not only down to opening a means of communication with strangers but also the need to protect personal information and concerns about photographs of children being openly available online. With many of these sites photographs can be "tagged" meaning that they show the names of the people in the picture and even a link to their profile. It is worth talking to the parents of your child's friends in order to ensure they understand your own position on whether you are happy for your child to appear in any photographs they may post online.Instant Messaging

Instant Messaging is a means of communicating over the internet using text. What you type appears on the screen of the person you are "talking" to in real time. Many children use these tools to chat with each other. It facilitates:

- Person-to-person text messaging
- File transfer/sharing
- Audio chat
- Video conferencing
- Chat room messaging
- E-mail facilities
- SMS
- Gaming

It is possible to set limits in terms of who can speak to you or block users, simply look for the options or preference links on whichever messenger your child is using.

You can also set up your home computer to keep a record of the conversations that take place using Windows Live/Instant Messenger.

Skype

In order to lock out unwanted communications in Skype, you can set up privacy levels very simply. Just open Tools > Options > Privacy, and set your preferences for receiving communications. I would recommend you set Skype to only receive calls and chat from people you know and always keep the chat history forever.

You may also want to consider switching off the tool which shows your status online.

Supervising your child's time online

It is important that we take the time to understand what our children are doing online and that they understand that their activities are being monitored in the same way their behaviour would be in other situations. Striking the balance between allowing the children sufficient independence and

monitoring their internet use can be a difficult one to strike but it is important to put these measures in place.

Your children should understand that, in order to ensure their safety, you will:

Regularly check their internet and search histories. To do this simply press CTRL & H when the internet browser is open.

Ensure that the computer is in a public area of the house. I urge parents not to place internet ready computers in children's bedrooms but rather to have them in the lounge or another commonly used room. No surfing without a lifeguard!

Set times during which the children can access the internet to ensure that it does not interfere with homework, exercise etc.

Hold a copy of their contacts list for email or messaging and be consulted before any new contacts are added to this list.

Share the measures you are taking with the parents of your child's friends in order to ensure they understand the rules. It can be a much simpler process if your child's friends are subject to similar restrictions.

Check your child's own websites to ensure that the content is suitable. Some parents may also wish to regularly check their child's email account for the same purpose.

Commercial parental control software

For those of you who wish to purchase additional tools a range of options are available. My advice is to test out a few options on a free approval period and speak to friends and family about their experiences with different solutions. Some commonly used packages are:

Cybersentinel

Net Nanny

CYBERsitter