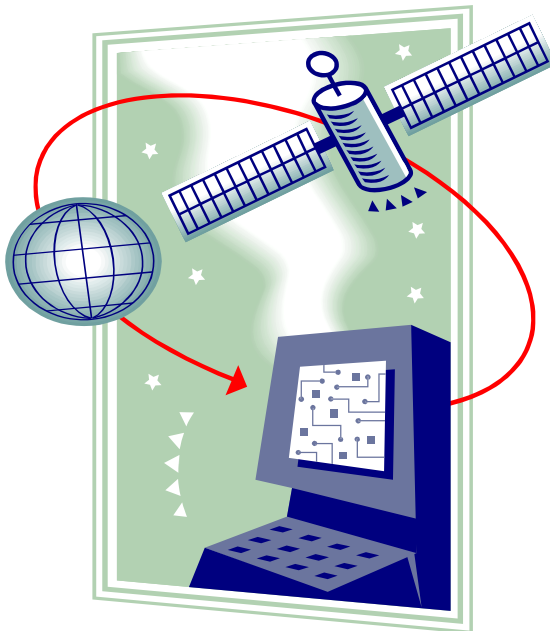




Singapore American School

Parent Guide to Digital Citizenship in the Internet Age



Dear Parents,

The Internet is an important place to work, play and learn for both adults and children. With our Blackboard e-learning system and our online grading information provided via PowerSchool, the Internet is not only a valuable educational and entertainment tool for your child – it is an essential home/school communication tool as well. In addition, many of the SAS information and research resources (library catalog and databases, video and animation sources, etc) are *only* accessible online. Therefore, it is an expectation that students have access to the Internet from home, while we provide them filtered access at school.

At the same time, parents and educators are concerned about the risks kids face online. The challenge is to stay current on what these risks are and how best to educate our students to deal with them. Through thoughtful engagement and direct instruction, parents and teachers can help students learn to be respectful and responsible digital citizens.

This booklet has been compiled to assist you in your efforts at home. It covers the following topics:

- General Online Safety Tips for Parents
- General Online Safety Tips for Teens
- Social Networking Safety
- Cyber-Harassment
- Downloading Music & Videos
- YouTube and Video-Sharing Sites
- Spam, Phishing and Malware
- Resources for Parents

We hope you find the information useful.

Last Update: September 2009

General Online Safety Tips for Parents

1. Keep your personal information safe – this is equally important for parents as it is for children. Giving out your personal details online should be done with *great* caution.
2. Keep your computer system up-to-date with patches and service packs (turn on auto-update features, but do manual update checks as well).
3. Install Internet security tools – antivirus, firewall and anti-spyware software (see the Resources for Parents section for more info). Update them often so your protection is current. Do not simply rely on their ‘live update’ (self-updating) features entirely; check them regularly to verify that they are in fact getting updated. Some spyware infections can disable these features without you even knowing.
4. Keep the computer in a public area of the house if at all possible. Invite your child to use their laptop in your living room or other public space. This way you can monitor what is happening when he/she is online. Knowing you are watching, kids are less likely to put themselves in risky situations and you can safely oversee what's going on.
5. Make sure your child doesn't spend all of his or her time on the computer. People, not computers, should be their best friends and companions. Help them find a balance between computing and other activities.
6. Take an interest in your child's online activities – Learn enough about computers so you can enjoy them together. Encourage discussions between you and your child about what they enjoy online. If you want to know more, get them to teach you.
7. Get to know their "online friends" just as you get to know all of their other friends.
8. Establish Internet ground rules and hold them accountable if they do not comply.



General Safety Tips for Kids

1. Never give out private information about yourself or your family online. This includes:
 - name – if you must give out names, use ‘screen names’
 - address
 - phone number
 - school
 - city
 - passwords
2. Don't fill out forms or questionnaires online – these are ways that predators or attackers may gather your private information.
3. You are going to run across things on the Internet that make you feel uncomfortable. Remember: some people use the Internet for bad things. Be cautious and wary. Don't believe everything you see or read either. There is a lot of false information out there.
4. Never make plans to meet online buddies without talking it through with your parents.
5. Don't open up e-mails, files, or URLs (web addresses) sent to you by people you don't know or trust.
6. Don't do anything that could cost your family money unless your parents are there to help you do it.
7. Always follow your family's Internet ground rules.
8. Share what you're doing online with your parents and teach them – they are interested and they need your help to understand your world online.
9. Be guided by these three words when you chat, blog, or work on your Facebook or MySpace type of account: **Do No Harm.**



Social Networking Safety

Social Networking Sites are web services designed to help users find and connect to friends. These sites began as simple blogs. However over the past several years, S.N. sites have gained more and more features, and now include the ability for users to fully customize the look, feel and navigation of their pages, while being able to post photos, video, music and other files along with the standard journaling capabilities. They are designed for sharing and incorporate additional features which help users link up with friends, and friends of friends, and friends of friends of friends...

The most popular one currently is Facebook. However, there are very many of them and all sport slightly different feature sets. Importantly, these sites are not at all about privacy – and yet many users post very private information on them. There is a false sense of security regarding Facebook and other S.N. sites, and many kids believe that only their friends are viewing them.

A very good source of information about Facebook Security, complete with suggestions and instructions, is available here:

<http://www.sophos.com/security/best-practice/facebook.html>

Additionally, the following S.N. safety tips are courtesy of Parry Aftab, Executive Director of WiredSafety.org:

The quick tips for tweens and teens:

- Put everything behind password protected walls, where only friends can see.
- Protect your password and make sure you really know who someone is before you allow them onto your friends list.
- Blur or morph your photos a bit so they won't be abused by cyber bullies or predators.
- Don't post anything your parents, principal or a predator couldn't see.
- What you post online stays online - forever!!!! So thinkb4uClick!
- Don't do or say anything online you wouldn't say offline.
- Protect your privacy and your friends' privacy too...get their okay before posting something about them or their photo online.
- Check what your friends are posting/saying about you. Even if you are careful, they may not be and may be putting you at risk.
- That cute 14-year old boy may not be cute, may not be 14 and may not be a boy! You never know!
- And, unless you're prepared to attach your Facebook to your college/job/internship/scholarship or sports team application...don't post it publicly!

...And for parents:

- Talk to your kids – ask questions (and then confirm to make sure they are telling you the truth!).
- Ask to see their profile page (for the first time)...tomorrow! (It gives them a chance to remove everything that isn't appropriate or safe...and it becomes a way to teach them what not to post instead of being a gotcha moment! Think of it as the loud announcement before walking downstairs to a teen party you're hosting.)
- Don't panic...there are ways of keeping your kids safe online. It's easier than you think!
- Be involved and work with others in your community. (Think about joining WiredSafety.org and help create a local cyber-neighborhood watch program in your community.)
- Remember what you did that your parents would have killed you for had they known, when you were fifteen.
- This too will pass! Most kids really do use social networks just to communicate with their friends. Take a breath, gather your thoughts and get help when you need it. (You can reach out to WiredSafety.org.)
- It's not an invasion of their privacy if strangers can see it. There is a difference between reading their paper diary that is tucked away in their sock drawer...and reading their Facebook. One is between them and the paper it's written on; the other between them and 700 million people online!
- Don't believe everything you read online – especially if your teen posts it on her Facebook!
- And, finally....repeat after me – “I'm still the parent!” If they don't listen or follow your rules, unplug the computer...the walk to the library will do them good. ☺

For more information, please visit <http://www.wiredsafety.org/>



Cyber-Harassment

The following definition and other information are excerpted from StopCyberbullying.org, one of the WiredSafety.org family of websites:

"Cyberbullying" [Cyber-Harassment] is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet... or mobile phones. It has to have a minor on both sides, or at least have been instigated by a minor against another minor. Once adults become involved, it is plain and simple cyber-harassment or cyberstalking... The methods used are limited only by the child's imagination and access to technology. And the cyberbully one moment may become the victim the next. The kids often change roles, going from victim to bully and back again.

Cyber-Harassment can take place in a variety of ways, and typically is more of a problem in Middle School, but those most commonly experienced at SAS include the following:

- Impersonation – fake accounts set up in a victim's name, then outrageous and hurtful things said to contacts, inciting conflict among friends.
- Harassment via SN, IM or SMS – typical verbal bullying
- Malicious statements, information or 'Photoshopped' photos of victims posted on blogs, social networking sites or web sites.
- Invasive or compromising pictures taken of victims with cell phones and sent out to others, causing hurt and embarrassment.
- Internet Polling or Surveys ("Who's Hot and Who's Not?" or "Rate these girls/guys") – often posted on blogs or web sites but also distributed via email or Facebook.

The School's role in dealing with cyberbullying which occurs off-campus and outside of school hours is a bit of a grey area, however, our support, guidance and concern for students developing into responsible citizens does not stop at the school gates. Students engaged in acts of digital bullying may be held responsible under school disciplinary guidelines. This is true especially when other SAS students are involved, and the action off campus affects the climate or learning of students on campus.

Parents need to be the one trusted place kids can go when things go wrong online and offline. Yet they often are the one place kids avoid when things do go wrong online. Why? Some parents tend to overreact. Most kids will avoid telling their parents about a harassment incident fearing they will only make things worse (calling the other parents, the school, blaming the victim or taking away Internet privileges.) Unfortunately, they also sometimes under-react. Parents need to understand that a

child is just as likely to be a cyberbully as a victim of cyberbullying and often go back and forth between the two roles during one incident.

Tips for Dealing with Cyber-Harassment:

- Talk to your child about their communications and actions online, and teach them ways to prevent themselves from being inadvertent cyber-harassers.
- Teach your child not to stand by and allow harassment of any sort, and not to ignore it when others are in pain or being harassed.
- Kids should Stop, Block and Tell if they are victims of cyber-harassment:
 - Stop! – Don't do anything; take some time to calm down rather than reacting in kind.
 - Block the harasser or limit your communications to close friends.
 - Tell your parents, counselor or teacher.
- Take screenshots of malicious web sites or blog postings as evidence in case it is required at a later time. (Press Alt+PrintScreen on a PC, then paste the screenshot into a Word document or new image editor document; Shift+Cmd+3 on a Mac will save the screenshot as a PICT to the desktop).
- Print or save to file the text log from your IM chat session (this feature must be turned on first – see the Preferences in your chat client to enable logging of conversations). As in the point above, the log may be necessary as evidence at a later time.
- Practice safe and considerate use of the Internet - see “Ms. Parry’s guide to correct online etiquette (Netiquette)” here:

http://www.stopcyberbullying.org/take_action/msparrysguidetonetiquette.html



Downloading Music & Videos

Does your child download music and videos online? It's important that you know. Find out whether they are sharing files from your computer and check out the software they are using, if they are doing so. Learn how it's done, do it with them, check the settings in the software so you know which folders on your computer are exposed to the world.

There are many ways your teen may be accessing music for free via the Internet. Skype and other IM/chat clients make it easy to send/receive large files such as mp3's and videos to/from friends. S.N. sites allow users to easily post and share files among their friends. File sharing software (aka P2P – “peer to peer”) such as the many BitTorrent clients are free to download and use. A lot of parents aren't even aware that their children have installed them, nor the risks they pose. Aside from music and videos, P2P clients also open your computer up to the danger of malicious files (viruses, worms, Trojans, spyware). That aside, there are legal implications to the sharing of music and videos. Singapore is cracking down on illegal piracy and the sharing of music and videos, and you and your child may be at risk. It's important to know the facts.

Teens need to understand that sharing music online without paying for it is illegal. Whether you agree with that or not, it is currently the case. While this issue continues to drag through courts around the world, at present it is generally against the law. This is a difficult thing for teens to accept because “everyone is doing it” – even many adults. Maybe even you.



Discussion Points For This Issue:

Aside from discussing the legal risks, perhaps another way to approach it is to discuss the impact their downloading and sharing has on other people – particularly the artists and those who work in the entertainment and retail industries:

1. **Plagiarism and the Illegal Use of Intellectual Property** – teens need to learn to respect the property of others. Most kids understand that plagiarizing a book or article is wrong, but have more difficulty relating this concept to music downloads. While it is legal to rip tunes from a CD that they have purchased for their own use on their mp3 player, sharing them is also a form of plagiarizing. The artist has not granted permission and does not receive compensation for the use of their intellectual property.
2. **The Impact on the Workforce** – Downloading has had a huge impact on the entire music industry. While it might not bother you too much that the large music labels have had to become more lean, competitive and responsive to the changing market, the effect on all the supporting people involved in CD production – from songwriters, to producers, to graphic designers, to session artists, to public relations and advertisers, to retailers – has been disastrous. Declining CD sales have caused many retailers to go out of business, and many of the CD production supporting roles have diminished. This means fewer and fewer jobs. The impact on these people and their families is huge. Many of the retail jobs are part-time, staffed by teens and young adults. If these jobs disappear, then it may have a direct impact on your child when he/she needs to find part-time employment. Some of the supporting roles in CD production represent entire careers that have been wiped out too, not simply part-time work. These avenues may also be closed for your teen. One thing is for sure, downloading and sharing of music illegally over the Internet is certainly not generating lots of new jobs for young people.

For more comprehensive info on this topic, see:

http://www.wiredsafety.org/law/copyrights/riaa/downloadingmusic_parryguide.html



YouTube and Video-Sharing Sites

The past two years have seen a huge surge in the popularity of video-sharing sites, fueled mainly by the success of YouTube.com. All of the major social networking sites have incorporated this capability within user accounts. These “video-networks” allow anyone to easily upload and share videos that they create, and users can watch, copy or link to them. Even video taken on cell phones find their way onto these sites, meaning that literally *anyone* can do it. It doesn’t require expensive equipment to produce the videos.

Most of these sites have some sort of acceptable use policies that define what users can and can’t post. For example, copyrighted materials such as DVD movies are not allowed but hardcore pornography may be, although only in an ‘Adult’ section of the network. It’s important for parents to get up to speed on the kinds of things their children are able to view online.

As with the S.N. sites, the video networks may require some sort of registration to become a user. However, despite posted age restrictions, there are no age verification systems in place to prevent younger users from lying about how old they are. These sites rely on the honor system and self-policing because there are literally millions of members. The companies are not able to deal with the membership volume in any realistic and personal way. Therefore, objectionable and offensive material regularly finds its way onto the networks and it takes time before the administrators can remove it, if ever.

The following is excerpted from an article by Parry Aftab, Executive Director of WiredSafety.org:

How graphic does the video get?

How graphic do you want? There are documented incidents of graphic combat video from the Iraq war, be-headings, pornography, graphic fights, pedophilia and other highly objectionable material posted to the various sharing sites.

What are the potential risks?

Let me count the risks. Young children react in different ways to explicit videos. Older teens can be affected as well. Not to mention the potential for video-bullying... situations that were caught on tape and now available for the entire world to see. The affect this has on the target of the bullying can be immense. There are also situations where internet predators have coerced, badgered or even black-mailed young victims they have found online to perform various sex acts on camera and then send it to them. They used the threats of something bad happening to them or someone they loved if they didn’t play along. Most of the

time these predators have managed to isolate these kids from their families, who typically are totally unaware of what is going on in their own households.

For more info see: <http://www.wiredsafety.org/resources/pdf/1%20Tube.pdf>

Tips for Dealing With This Issue:

- As already mentioned in the *General Online Safety Tips for Parents* section, be sure that you are aware of what your teen is doing online. Take an interest in their activities on the computer.
- Encourage use of computer is in a public area of the house, not your teen's bedroom.
- Watch some of the videos with your teen and talk to him/her about the potential impact on viewers, and on the people involved in the video. Many of the videos are interesting, informative, funny and entertaining. Some of them are openly offensive. Your teen can easily tell the difference among them. However, sometimes the 'funny' ones are at someone's expense, or may be used for blackmail and other harmful purposes. Kids need the tools to be able to discern this kind of thing for themselves. It's not easy, but sheltering them from it will certainly not give them the opportunity to gain the necessary tools.



Spam, Phishing and Malware

Your computer is under the constant threat of attacks from hackers and data miners who have a variety of nefarious purposes. This section defines and discusses the main categories of these threats. See the *Resources for Parents* section for more information and help.

“Spam” (junk email) continues to flood the Internet. Some studies estimate the spam to legitimate email ratio to be as high as 4:1. Aside from the annoyance of spam, the real issues it poses are 1) load on networks and email servers, and 2) scams. Scams on the Internet are rampant and gaining more sophistication. It used to be easy to discern a spam scam by the poor writing, grammar and/or spelling. This is no longer the case as the scams seem more and more legitimate. Users run the risk of being sucked into great financial loss. Whenever you receive something that seems fishy, do your research. Google the subject line of the spam or keywords in the body of the message to verify that it’s not a scam. There are a number of good resources online to help you do this, and there are software tools that can filter out spam to a large extent.

“Phishing” refers to the attempt to fraudulently acquire sensitive information such as passwords or credit card details through email or other electronic communications. While simple email advertising can be considered spam, spam in the form of phishing poses a greater threat to users. As with the scams noted above, do your research! Avoid clicking on any links in a spam message unless you know exactly what the source is and what the consequences are.

“Pharming” is a growing problem and is defined as a hacking attack which aims to redirect a website’s traffic to another (bogus) website. Most often this attack is generated by unwittingly installing spyware. The bogus website often masquerades as the real site, thus lulling users into supplying sensitive information. Pharming is a concern not only to users but also to e-businesses and online banks. There are ways to detect the pharming attempts, but general vigilance and due caution is appropriate for all users.

“Spyware” is a major threat that all users face online. Spyware can be defined as a broad category of software designed to intercept or take partial control of a computer’s operation without the informed consent of the user. One type of spyware called a ‘keylogger’ records what a user types in order to intercept sensitive information such as passwords and credit card details. Other spyware is designed to deliver unwanted advertising to a user’s desktop in the form of ‘pop-ups’. Spyware is sometimes installed as extra payload along with other software installs, particularly P2P software. Often, spyware is picked up as a ‘drive-by download’ from a website that you or your child visits. Spyware is almost always a *stealthy install*, happening without user interaction or knowledge.

A “Virus” is a small bit of computer code that has the ability to replicate itself onto other files with which it comes in contact. A virus is not a complete program in and of itself. It contains a series of methods or procedures which may alter the behavior of some other program, or launch actions on its own once it has infected a host computer. These actions can be as serious as wiping out an entire hard drive. Viruses are usually triggered by a user response (ie. the user must double-click to launch it, or perform some other action which triggers it) and their behavior is usually not even visible to the user.

A “Trojan Horse” is a type of malware which portrays itself as something other than what it is at the point of execution. It may advertise its activity after launching, but this information is not apparent to the user beforehand. Unlike a virus, it neither replicates nor copies itself, but causes damage or compromises the security of the computer when triggered. Trojan horses must be sent by someone or carried by another program and may arrive in the form of a joke program or software of some sort.

A “Worm” (aka “email worm”) is the most destructive and pervasive malware problem on the Internet. A worm distributes by copying itself using email or another transport mechanism. Worms typically arrive on a computer via exploitation of a system vulnerability (such as a browser security flaw) or by clicking on an infected e-mail.

Tips for Dealing with Malware Threats:

- The best defense is a strong offense. It is *essential* to:
 - Purchase and install an Internet Security Suite which contains a good firewall, anti-virus scanner and possibly a spam blocker. Keep the software up-to-date with patches, upgrades and virus definitions.
 - Purchase and install an anti-spyware scanner. Keep it up-to-date with patches, upgrades and spyware definitions. (Many Internet Security Suites now include anti-spyware scanners.)
 - Run these tools once a week.
- Don't open but delete files or messages that look suspicious. Pay close attention to message sources. Research the subject lines if you aren't sure.
- Beware of P2P software, or uninstall it if you already have it – there will be extra bits of software that came with the original install that may be difficult to find or remove. Do your research. Someone on the Internet will provide tips for how to get rid of all the pieces.
- Teach your child to be very selective about sites he/she visits. Sweep (run an anti-spyware scan of) your system, and then have your child visit a popular website. Immediately sweep your system again to see if the site installs spyware. Make note of the sites that do and ban them.

Resources for Parents

General Online Safety Info for Parents and Teens:

- On Guard On Line - <http://onguardonline.gov/>
- WiredSafety.org - <http://www.wiredsafety.org/>
- GetNetWise.org - <http://kids.getnetwise.org/safetyguide/teens>
- Center for Safe and Responsible Internet Use <http://csriu.org/>

Social Networking Sites:

- Facebook.com - <http://www.facebook.com/>
*There are MANY. Google “social networking” or ask your son or daughter which ones are popular right now.

Internet Scams & Phishing:

- AntiPhishing.org - <http://www.antiphishing.org/>
- US Securities and Exchange Commission Internet Fraud Page - <http://www.sec.gov/investor/pubs/cyberfraud.htm>
- FBI Internet Fraud Page - <http://www.fbi.gov/majcases/fraud/internetschemes.htm>
- NCL Internet Fraud Watch - <http://www.fraud.org/welcome.htm>
- Internet Scambusters - <http://www.scambusters.org/>
- Hoax-Slayer.com - <http://www.hoax-slayer.com/>

PC Security:

- Symantec Security Response Center (virus and malware info): http://www.symantec.com/home_homeoffice/security_response/index.jsp
- Microsoft Consumer Online Safety Education - <http://www.microsoft.com/protect/>
- Internet Security Suites and Anti-Spyware Scanners – lots available. Some popular ones:
 - Norton Internet Security Suite & other tools - <http://www.symantec.com/>
 - Zone Alarm Internet Security Suite - <http://www.zonealarm.com/>
 - McAfee Internet Security Suite - <http://www.mcafee.com/>
 - Kaspersky Internet Security Suite - <http://www.kaspersky.com/>
 - F-Secure Internet Security - <http://www.f-secure.com/>
 - Spy Sweeper - <http://www.webroot.com/>
 - Spyware Doctor - <http://www.pctools.com/>
 - Ad-Aware - <http://www.lavasoftusa.com/>

Notes