

The School's Policy on Internet Safety.

The School does not filter Internet content because software-based filters are not Effective in blocking objectionable material from children and yet block a substantial amount of benign content. This can result in complacency on the part of the responsible adults (parents or teachers). Meanwhile the individual child learns nothing about what they should do when they encounter materials that are inappropriate or make them feel uncomfortable; the opportunity for safe discussion about such content is lost. Ultimately, this is a disservice to the child.

We approach the issue of inappropriate Internet content (or any inappropriate content) as one of trust and individual responsibility. The expectations are discussed in the beginning of the year (usually when classroom charters of behavioral expectations are being formulated) and reminders are made throughout the year. We go an extra step with Grades 4 through 8 with an agreement (AUP) that is signed by student and parent, where each accept such responsibilities. Our philosophy is to prepare our students for the reality of the Internet (its good side and its bad) rather than present a partially sanitized version that exists only at school. It is our hope that parents share our expectations of responsibility and serve as that trusted person when questions do arise. We do filter email for spam. Since spam is typically unsolicited, we treat it differently than we do inappropriate content on websites. We caution students to never enter their actual email address or name on any website (the source of where most spammers get their email addresses). Inevitably some will enter their address, but our spam filter will catch the worst (hopefully) of what results. Spam filters are not perfect, but are generally much more effective than content filters.

There are many other things to be concerned about such as identity theft, inappropriate solicitations/meetings that result within chat rooms and personal details posted to so called social networking sights (ie. myspace, club penguin). As students get older, phishing (gathering personal data by duping an individual in to thinking they are providing the data to a trusted source) will undoubtedly become more of an issue as it is now for grown-ups. Content filtering addresses none of these issues.

All of these issues have considerable relevance today and we take them very seriously. The School will continue to review its efforts to ensure the safety of all of its students, on and off line. It is a partnership.

Sample Tips

- Clear, simple, easy-to-read house rules should be posted on or near the computer.
- Talk to children about what personal information is and why you should never give it to people online.
- Let children show you what they can do online, and visit their favorite sites.
- Children's screennames should be nondescript so as not to identify that the user is a child.
- Talk to children about what to do if they see something that makes them feel scared, uncomfortable, or confused.
- Keep the computer in the family room or another open area of your home.
- Web sites for children are not permitted to request personal information without a parent's permission.

