



Ref: USS/Cir/ 664 /2011

Date: 24/08/2011

**For Circulation to parents only**

Dear Parents,

We had organized an interactive session on 27/08/2011 at 11:00 a.m. for the parents. The PEP was mentioned in the students handbook and planner. Our endeavor is to provide and opportunity to all of us, parents and teachers to get and insight on issues and concerns. During the session on Saturday 27/08/2011, PTA had invited Mr. Vicky Shah, an expert in cyber crime (contact Mr. Vicky Shah on +919820105011 from 11: hrs to 17:00 hrs during weekdays or write to him on [Vicky@cybercrimes.in](mailto:Vicky@cybercrimes.in) or [Vicky@theeagleeye.in](mailto:Vicky@theeagleeye.in) . it is a pity many of the parents missed this wonderful opportunity. Since the session involved issues that affects all of us in one way or the other. We are providing you with additional inputs.

The Internet in Utpal Shanghvi School is available for your student's use and we believe it will be a great tool for instruction and research. In order to assure a safe environment for your student, we have implemented technology (Firewall Internet total security) at our school to further safeguard your ward's safety when using the Internet.

We have installed a comprehensive Internet filter so that all Internet use at the school is monitored, filtered and reported. The School uses technology protection measures to block or filter, to the extent possible, access of visual depictions that are obscene, pornographic, and harmful to minors over the network.

Access to any sites deemed inappropriate, is completely blocked. In addition, adults are always present and monitoring students anytime they are logged on. This is a regulatory requirement as per the Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008.

We recommend that you too establish a similar Internet use policy at your home and that you discuss safe and appropriate Internet use at home and at school with your ward. We wish our students use technology for the optimum academic purpose and avoid any inconveniences for self, and the institution. We have included some tips for parents with this letter to help you establish a safe Internet environment at your home.

Yours faithfully,

(abha dharam pal smt.)

Principal.

Encl.: As above

adp/sak

**From the Principal's Desk :**

**Why Schools Need a Strong Internet Security Policy and Controls**

Developing a strong and comprehensive internet security is the important first step in managing school Internet access. This is to ensure the infrastructure and facilities provided by the school are governed in the right perspective and a culture of Internet hygiene is created among students. Our security also includes equipment and devices owned by the school as well as those brought onsite by students and/or teachers and other staff (this includes and does not limit to external storage devices).

In addition to the many advantages offered by easy Internet access, the threats delivered via the Internet must be addressed. Schools need to protect their students and employees and safeguard networks from various known and unknown threats, risks and vulnerabilities.

These Internet protocols provide ways for students and others to share and/or download files from the Internet. They not only threaten to expose your networks to viruses and malware, they can lead to exposure to inappropriate content or legal problems in the case of copyrighted materials. This is a big challenge and we need to ensure our students do not fall prey to such legal implications.

**The use of an Internet is a privilege, not a right, and misuse may also lead to disciplinary and/or action from School authorities** as well as Law Enforcement Agencies.

An effective **SECURITY** serves as the critical first step in securing school's Internet access and protecting school from Web-based threats:

School authorities may use email to communicate with parents and students.

**Inappropriate Content** – Students can be exposed to a variety of damaging material delivered via the Internet. Schools are ethically and legally responsible for governing and safeguarding children from pornographic, racists, violent and other offensive Internet Contents.

**Social Networking Sites** – Websites such as MySpace, Orkut, Ibibio and Face book can easily distract students from their work and even expose them to online predators. These sites offer various lucrative schemes which may result in children's misbehavior and mischief.

**Cyber Bullying** – Without strict guidelines and enforcement, students with Internet access may become victims of cyber bullying, a growing threat to their well-being and safety. These may result into mental imbalance among children's.

**Safeguarding School Networks** – Internet threats such as malware, viruses, anonymizers, and other unwanted agents can be accidentally or intentionally introduced by users, causing serious damage to school networks and systems. These may also harm other computer systems and networks outside school premise. The onus will be on the user and hence the need to protect the user and the school from such unavoidable risks.

## **Managing Your Students' Online Behavior**

As educators, we are responsible for maintaining a safe Internet learning environment for the children we teach. This means protecting the students from damaging content, online predators, cyber bullying or even distractions such as social networking that erode the rich learning environment you are trying to maintain. By creating a comprehensive internet security we can assure that the Internet is a valuable learning tool and not a dangerous diversion. The idea is create cyber ethical guidance among students for better digital society.

### **Block Inappropriate Sites**

School computers prohibits from being used to view, download, upload, forward, print copy or file any content which deem inappropriate. This includes and does not limit to sexually explicit material, social network sites, or any other non-learning related Web content. This will also help safeguard our networks and systems by banning intensive sites that offer music, games, shopping or streaming audio and video.

Causing harm to others or damage to the property, such as:

1. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
2. Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
3. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
4. Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
  1. Using another's account password(s) or identifier(s);
  2. Interfering with other users' ability to access their account(s); or
  3. Disclosing anyone's password to others or allowing them to use another's account(s).
5. Students shall not reveal on the Internet personal information about themselves or other persons. For example, students should not reveal their name, home address, telephone number, or display photographs of themselves or others, Students shall not meet in person anyone they have met only on the Internet

### **Internet Tips for Parents**

- Become more computer literate so you can learn how to block objectionable material.
- Keep the computer in a common area in your home, where you can watch and monitor you child.
- Monitor your child's email by sharing an email account
- Make your child's favorite sites easy to find by bookmarking them
- Take time to go online with your child so he/ she can develop healthy online behavior

- Block dangerous or threatening sites, such as private chat rooms, with safety features provided by your ISP (Internet Service Provider) or install a firewall solution.
- Be aware and inform your child that anything posted on the Internet is there forever. Also anytime they post something on a blog, they are revealing their email address.
- Be on the lookout for any unfamiliar charges to your credit card and/or phone bills, which could indicate online activity involving your child
- Be sure you are aware of any Internet access your child has away from home. Find out if safety features are in place at your child's school, after-school center, friends' homes, or any place where he or she could use a computer without your supervision.
- Don't ever dismiss your child's concerns while online. If your child reports feeling uncomfortable about an online exchange, take him or her seriously.
- **Immediately forward copies of any obscene or threatening messages you or your child receives to your Internet service provider.** (DO NOT FORWARD TO ISP (Internet Service Provider) INSTEAD REPORT TO LAW ENFORCEMENT if the need be.) Forwarding obscene or threatening message in itself is an offence; avoid getting involved in the same.
- If you are aware of the transmission, use, or viewing of child pornography online or if your child has received child pornography via the Internet, contact your local law enforcement agency
- Many sites use "cookies," devices that track specific information about the user, such as name, email address, and shopping preferences. Cookies can be disabled. This could be set through your internet browser settings.

#### **Rules for Your Child**

- Follow the rules set by your parents, as well as those set by your Internet service provider.
- Never trade personal photographs in the mail or scanned photographs over the Internet.
- Never reveal personal information, such as address, phone number, or school name or location.
- Use only a screen name and change it often.
- Never agree to meet anyone from a chat room in person.
- Never respond to a threatening email or message.
- Always tell a parent about any communication or conversation that was scary or made you uncomfortable.