Bal Bharati
PUBLIC SCHOOL
Sector – 21, Noida
Phone : 0120-2534064, 2538533 / E-mail :bbpsnd@balbharati.org
Website : http://bbpsnoida.balbharati.org

EXPLAINING CYBER RISK / SECURITY & SAFETY

A : CYBER SAFETY

According to 'Online Victimization: A Report on the Nation's Youth,' a recent study conducted for The National Center for Missing and Exploited Children (NCMEC).

- One in 20 has potential financial threat.
- One in four regular Internet users younger than 17 is exposed to unwanted sexually oriented pictures online during the past year.
- One in five youths received an online sexual solicitation or approach during the past year.
- One in 17 was threatened or harassed online during the past one year.
- One in 33 received an aggressive sexual solicitation online involving offline contact or a request for offline contact during the past year.

What might those statistics mean in real numbers? Quite a lot-- almost 24 million youths between the ages of ten and seventeen used the Internet regularly last year and the number is multiplying everyday.

WHAT IS CYBER SECURITY?

Cyber security is a branch of technologies, processes and practices designed to protect networks, computers, programs and data from attacks, damages or unauthorized access.

The concept of Cyber security has become very relevant as the users of these devices are prone to direct or an indirect attack in a friendly or not so friendly way from those who have intentions to exploit them physically, financially, on account of terrorism or to the extent beyond imagination of these individuals.

TYPES OF CYBER RISKS:

Cyber risks can be divided into three distinct types:

- **Cyber Crime**
  Conducted by individuals or organized groups. The intent of Cyber criminals is extracting money, data or causing disruption. Cyber crime can take many forms, including the acquisition

of credit/debit card data and intellectual property, and impairing the operations of a website or service.

- **Cyber War**
  A nation or a state conducting a sabotage or an espionage against another nation in order to create a law and order problem or to disrupt economy.

- **Cyber Terror**
  An organization, working independently of any nation or a state, conducts terrorist activities through the medium of cyberspace.

MAJOR ISSUES:

- Almost every child in the urban or semi urban society is hooked to the internet;
- These children start using internet as early as the age of 7yrs;
- Children by nature are very inquisitive and thus, try everything new;
- The Internet offers them a world of glamorous opportunities;

AND THESE INNOCENT MINDS ARE UNAWARE OF THE RISKS INVOLVED SUCH AS:

- Inappropriate conduct
- Inappropriate content
- Inappropriate contact

THERE IS A GENERAL LACK OF AWARENESS ABOUT:

- **Cyber threats;**
- **Safe online habits;**
- **Legal provisions dealing with cyber space;**

All this makes children a potential victim of Cybercrime.

WHICH IS THE APPROPRIATE AGE FOR KIDS TO ACCESS ONLINE SERVICES?

Children live and breathe this environment as “digital natives”. Excluding them from the digital world could prove to be a disadvantage for their development.

We, therefore, need to ensure that minors are able to use online services under **adequate supervision of their parents and teachers** and are even further protected with the help of suitable safety tools, such as parental controls, as well as adherence to good practices. Remember, children normally access those online services – such as social network or other adult oriented sites which have not been developed for them. Also services, such as email, prohibit children under the age

of 13 from creating an account. However, in both cases, no mechanisms have been put in place to enable the user's age to be verified, given that any date of birth can be used to fulfill the requirements. Additionally, the **checks used can be easily sidestepped**. The main reason why **children under 13 are not allowed** to have an email address or a social network profile is the **law protecting a child's privacy**, commonly known as COPPA (Children's Online Privacy Protection Act), which companies have to comply with.

So, there is an urgent need to inculcate safe online habits. Since Internet is a reality & cannot be wished away and you cannot block sites exclusively for the children, so-

- **Children must learn how to Pause & Think before they connect online.**
- **Children must learn to be safe and alert on the Internet.**

The Mantra of online safety is 'Pause & Think before you Connect !'

When I say PAUSE it means :

Ask yourself these questions:

- Do you know and trust the persons you are dealing with ?
- Do you understand the implications of what you are sharing and downloading?
- How will you feel if your information ends up somewhere you didn't intend?

In the answer to these questions lies your online safety.

PRECAUTIONS, OUR CHILDREN MUST TAKE !

- **Limit your online friends to people you already know.**
- **Change privacy settings to restrict who can see and post on your profile on Facebook, Whatsapp etc. Don't stick with the defaults.**

WHILE ONLINE …

- **Seek guidance before participating in any online activity.**
- **Most Apps are interested in your personal data.**
- **You decide whether they are worth the privacy loss?**

Don't think that Instagram, WhatsApp, Facebook or Snapchat are free. If you create your account on any of these social networking apps or, games, you are giving your personal data, chats, pics and personal videos to these companies which later on sell to the other companies for purposes like sending ads, schemes etc. Even from your chats, they analyse your taste, your interest and the group opinions about popular eating points, movies,

places, dresses, etc. Not only this, data is used by the entrepreneurs to expand or start a new business but can also become a real security threat for the user.

Children need to be aware of loading up PCs, tablets, phones, with applications that have not been approved or checked out.

Be careful on pop up messages like “you won” or “you will get free”, just ignore these messages.

While installing any app or software always read the instructions carefully.

GUIDELINES FOR SCHOOLS:

Schools must have a curriculum on digital citizenship and online safety. This is very important as the statistics of cyber bullying, stalking, sexting, scandals, predators, and privacy invasions continue to rise. It is vital for schools to address these issues and coach students through the Wild West of the internet. Also schools must -

- Develop programs to educate and inform children, students and parents about the opportunities and challenges of ICTs in learning programs.
- Monitor e-mail traffic and Internet use.
- Provide filters on school servers to help guard against access to inappropriate materials.
- Provide direction and advice about ICTs (including the Internet and mobile phones) use and misuse, such as bullyingand e-crime.
- Ensure appropriate supervision & monitoring
- Keep abreast of constantly changing Internet safety information and communicate regularly to all stake holders.
- Inculcate net etiquettes to the students from class I onwards.
- Plan various classroom activities to spread awareness on Cyber Security and Digital Citizenship

GUIDELINES FOR PARENTS:

HOW DO YOU KNOW IF YOUR CHILD IS BEING CYBERBULLIED?

- **Snappy answers and moods swings**
- **Deletes social network account**
- **Withdraws himself from friends and family in real life**
- **Dramatic physical changes**
- **Pretending to be sick and trying to avoid school**

STEPS TO BE TAKEN:

- Establish limits for which online sites children may visit and for how long.
- Remember that Internet technology can be mobile, so make sure to monitor cell phones, gaming devices, and laptops. Position the computer in such a manner that you can monitor all activities effectively.
- Surf the Internet with your children and let them show you what they like to do online.
- Know who is connecting with your children online and set rules for social networking, instant messaging, e-mailing, online gaming, and using webcams.
- Continually dialogue with your children about online safety.
- Inform your child that they need to tell you if they get any weird or upsetting messages while chatting.
- Do not permit your child to be left alone in cyberspace for long periods of time – this is when they are most vulnerable.
- Educate them about the risks of webcam. Videos that broadcast over the internet are permanently out there and can be saved by anyone for later viewing or distribution.
- Talk to them about the implications of posting inappropriate pictures, saying disparaging things about other people and anything else that could damage a reputation or ruin a friendship.

Educate them about the Indian Cyber Laws. They are stringent, impose strict penalties and can be quite unforgiving at times.

- Hacking email ids
- Creating a fake profile in the name of someone else
- Pasting pictures of known persons on objectionable sites
- Sending derogatory emails and messages are some of the activities that can invite legal action.
- Teach your child that everything that one sees on the internet may not be true.
- People may be different than what they claim to be on the internet

PARENTS ARE THE ROLE MODELS FOR THEIR CHILDREN AND THEY WATCH WHAT YOU DO. THUS, IF PARENTS WANT THEIR CHILDREN TO BE SAFE AND SECURE, THEY MUST CHANGE THEMSELVES.

B : CYBER POLICY

OBJECTIVE:

In today's world, we are surrounded by electronic gadgets everywhere. As an educational institution, it is the school's responsibility to provide Internet facilities and IT devices/equipment which will benefit student learning outcomes, and the effective operations of the school.

However, these technologies (some provided partly or wholly by the school and some privately owned by the staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximize the benefits of these technologies, while at the same time to minimize and manage the risks.

Thus, we need to have in place, rigorous and effective school Cyber Safety practices which are directed and guided by this Cyber Policy.

CYBERSPACE:

It is a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

Owing to the numerous benefits brought about by technology, the cyberspace is a common pool of resources used by students, citizens, businesses, critical information infrastructure and all stake holders.

Information Technology (IT) is one of the critical sectors that rides on and resides in Cyberspace.

We must provide a right kind of focus for secured computing environment and adequate trust and confidence in electronic transactions, software, services, devices and networks.

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural and the data exchanges in the cyberspace can be exploited for nefarious purposes.

ELECTRONIC CRIME (E-CRIME)

It occurs when computers, or any other electronic communication equipment or devices (such as mobile phones or the internet), are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

IT DEVICES/RESOURCES:

They include (such as desktops, notebooks, and tablets), storage devices (USB and flash memory devices, CDs, DVDs, floppy disks, ipods, MP3 players), cameras (video and digital cameras and web

cams), all types of mobile phones, gaming consoles, video and audio players or receivers (portable CD and DVD players), and any other similar technologies

TYPES OF ELECTRONIC CRIMES (E-CRIME)

1. **Fraud & Financial Crimes**: Computer fraud is dishonest misrepresentation of fact intended to cause loss. For example, bank fraud, identity theft, extortion, and theft of classified information.
2. **Obscene or offensive content**: The content of websites and other electronics communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be illegal.
3. **Cyber bullying**: content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties. Any comment that may be found derogatory or offensive is considered harassment.
4. **Threats**: Advertisements promising unrealistic products/services (adware) and software that intentionally causes harm (Malware)
5. **Cyber Terrorism**: A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer based attack against computers, network, and the information stored on them.

VISION:

To build a secured and resilient cyberspace for citizens.

Need of a Cyber Policy:

"To protect information and infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation."

BBPS NOIDA CYBER POLICY:

This policy applies whenever students are using Bal Bharati Public School Information Technology equipment, services and/or resources, whether such equipment, service and/or resources is being used at school or home.

1. Students must not eat/drink near the IT devices.
2. Must respect school equipment and should not indulge in moving the IT equipment and/or cables.
3. Students must not cause damage to any equipment. If they spot any damage, they must inform the teachers immediately.
4. Must not use flash drives or any other external media(Cell phone, hard disk, CD, camera etc.) for the purpose of
    1. Saving or transferring the work
    2. Installing new software without due permission from the computer faculty.

5. Viewing social media sites/registering on any website/downloading any material for use must be under the strict supervision of the teacher.
6. In the computer lab, Internet access is allowed only after permission from computer faculty and the computer faculty reserves the right to check the IDs of the users.
7. Students are not allowed to bring equipment such as iPad, iPod, PSP, mobile phones etc. to the school. Any such equipment confiscated from the students will be kept by the school.
8. Students must report incidents of Cyber Bullying and misuse of IT resources to their teachers/parents immediately.
9. Hacking emails of school staff or others.

WHAT HAPPENS IF A STUDENT BREACHES THE BAL BHARATI PUBLIC SCHOOL'S CYBER POLICY:

If you breach this policy, you will be subjected to Bal Bharati Public School Behavior Management Policy.

1. Minor breaches (like installing new software, accessing internet, connecting IT devices without prior permission of the concerned teacher etc.) of this policy will result in the suspension period of two weeks.
2. Major breaches (like cyber bullying, identity theft etc.) of this policy will result in the suspension period of up to ten weeks.

3. If you behave online in a manner that threatens the well being of another child, student, parent or member of the school community, even if this occurs off-site during or after the school hours, the Principal/VP/HM has the authority to take appropriate action.
4. When it is suspected that a personal electronic device such as a mobile phone is used to capture images of a crime (such as an assault), or contains any other evidence of a crime, the device will be confiscated and handed to the police.
5. If the Principal suspects an electronic crime has been committed, this will be reported to the Police Department. Where there is a further reasonable suspicion that evidence of a crime, such as an assault, is contained on a mobile phone or other electronic device such as a notebook, computer etc., and the device will be confiscated and handed to the investigating police officer. The police will determine any further action.
6. These actions may be taken even if the alleged incident occurs off site and/or out of school hours.

GUIDELINES FOR PARENTS:

1. Place the computer in an open area in your home – not in your children's bedroom.
2. Set clear expectations for your children, based on age and maturity.
3. Install parental control (content filtering) software.
4. Learn internet basics, be approachable and lead by example.

TIPS FOR PARENTS TO AVOID AND IDENTIFY CYBER BULLYING:

1. Discuss any changes in mood or behavior with them. If you concerned, help your child to stay connected to friends and family they trust.
2. Talk to your child about cyber bullying before it happens.
3. Be aware of what your child is doing online and explore it with them.
4. Keep the lines of communication open so your child will be comfortable talking about if something is worrying them. Help your child to develop the skills they need to interact online safely and respectfully online. Guide their online activities and help them learn to communicate appropriately with friends and family.
5. Help your child to block anyone who sends offensive content. Most social networking services allow users to block and report someone who is behaving badly.

"Cyber bullying won't stop if it is ignored – you can help by listening to your child and working with them to take control of the situation."

GUIDELINES FOR STUDENTS & PARENTS TO USE THE INTERNET SAFELY:

1. Don't give out personal information such as your address or phone number.
2. Do not share passwords, user names, account IDs or PINs with anyone besides your parents.
3. Do not share other people's personal information or say things that might violate the safety or rights of others, even if you mean it as a 'joke'.
4. Do not leave the ICT devices unattended.
5. Don't become online 'friends' with people you don't know.
6. Don't open emails or attachments from people you don't know.
7. Never arrange to meet someone in person who you have met online.
8. If anything you see or read online worries you, tell your parents/teachers about it.
9. Never give out personal details in messenger or in personal profiles.
10. Remember that people may not be who they say they are.
11. Don't send pictures to strangers.
12. Most reputable chat rooms allow you to block messages from a particular sender.
13. Be careful about who you share photos with.
14. Use social network's privacy settings so only your friends can see your stuff.
15. What you do not do in real life, don't do on the internet. This includes all kinds of cyber bullying using text, photos and videos.

PARENT AND STUDENTS ACKNOWLEDGMENT:

1. To gain access to Bal Bharati Public School Information Technology systems, student and parent(s) must read the policy, understand its contents, and sign and return this Parent and Student Agreement page to the school. You should keep the policy for reference.
2. This policy and agreement, along with the additions or amendments, will remain in force as long as the student is enrolled at Bal Bharati Public School, Noida.
3. If it becomes necessary to add to, or to amend any of the conditions of this policy, parents and students will be advised in writing via the school circular.
4. The policy is available for download from the school website.

PARENTAL ACKNOWLEDGMENT:

I have read and understood that Bal Bharati Public School Cyber-Safety Policy, and understand that student internet access is granted for educational purposes according to the conditions stated in this policy. I understand that the internet is a global network of computers, and that whilst Bal Bharati Public School will monitor the student use of the internet, it is not able to control the content, or restrict student access to all controversial or inappropriate materials. I agree that I will not hold the school responsible. _____ (student's name) to be granted access to the Bal Bharati Public School IT Systems, and to the Internet.

Name of the Student: _____

Parent's Name & Signature: _____ Date: _____

STUDENTS ACKNOWLEDGMENT:

I have read and understood the Bal Bharati Public School Cyber Safety Policy, and agree to abide by those rules and conditions. I understand that if I do not abide by this policy, my use of Bal Bharati Public School Information technology Systems will be suspended, and that I will be subject to the School's Behavior Management Policy and the possible repercussions.

Student's Name & Signature: _____ Date: _____

Note: All the parents and students should sign this document at the time of admission of his/her ward in Bal Bharati Public Schools, Noida.