Bal Bharati PUBLIC SCHOOL
Sector-21, Noida, G.B. Nagar

CYBER SECURITY POLICY

THIS POLICY APPLIES TO EVERY STAFF AND STUDENT AT BBPS, NOIDA

Reflecting on the over indulgence and dependence on the electronic gadgets (including mobile phone), CBSE, in July 2009, has termed them as sources of distraction which can also be misused.

Aiming to create meaningful learning atmosphere in the school and particularly in the Classroom, the school doesn't permit any student carrying any electronic article to the school. Non-compliance of the rules would be considered as an offence.

If a student is found in possession of it then the unauthorised electronic equipment would be confiscated and will be kept under school custody. Along with this, the school counsellor would also take parental undertaking from the parents, stating that the offence would not be repeated. The school looks forward to create an atmosphere wherein creativity and learning is nurtured and hence enabling holistic growth of every student.

CYBER POLICY

This policy exists to ensure that all BBPS staff and students follow certain basic rules with regard to internet use and use of IT in general. Its aim is to prevent students or staff coming to harm as a result of others accessing intolerant, extremist or hateful web sites. Also, it is here to protect students and staff from cyber risks. BBPS has the right to monitor electronic information created and/or communicated by students or staff using school computer systems / equipment's and networks, including e-mail messages and usage of the Internet.

CYBER SPACE:

- It is a complex environment consisting of interactions between people, equipment's, 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.

SAFE USE OF INTERNET

- Must receive permission from a member of staff before accessing the internet.
- Must access only appropriate sites for their work; any attempt to bypass filtering system or access social networking sites or chat rooms will be with the permission of a teacher for a work related item.
- Must not claim to be representing the school in an official capacity when using the internet or e-mail or website privately.
- Must not use any internet services to purchase goods or make any payments unless
- authorised otherwise.
- As the internet allows you to do more and more online, it is extremely important to be aware of the dangers and how to stay safe.
- Use social networks' privacy settings so only your friends can see your information.
- Never open an email from an unknown source – it may contain viruses that can harm a computer. And don't access or use files without the permission of owner.
- Don't send pictures to strangers or view pictures that strangers send you.
- Passwords should be kept private (except from parents).
- Always use the two-factor authentication for email and other important logins.

STRATEGIES FOR RESPONSIBLE & SAFER INTERNET

There's no such thing as "private" online. Anything posted can be seen by or forwarded to strangers. Must know what's okay to post. Teen years are full of self-expression and rebellion. Just make sure that your you know your rules about suggestive material or other content that may reflect poorly on you. This means no embarrassing or cruel posts, no hate speech or groups, no compromising pictures you wouldn't want the whole world to see. Be a good digital citizen. Online cheating is still cheating and flagging inappropriate content isn't tattling.

Encourage critical thinking. You should ask "who posted this? Why?" Thinking this way will help you find trustworthy information, and it will also help you avoid online scams that deliver spyware and viruses directly to your home. You should also think critically about your own posts. Learn to ask yourself, "Why am I posting this? Who will see it? Could it be misunderstood?" Stay in safe neighbourhoods. Just as you learn not to walk down dark alleys alone at night, you need to know how to avoid creepy places online.

Review your own habits carefully. Parents are the ultimate role models. Keep channels of communication open.

Better safe than sorry. Make sure you are comfortable telling your parents/teachers if anything menacing or cruel happens - - no matter what site you were on.

- Never give out personal details like in messenger or in personal profiles.
- Never give a friend's details and never share your password with anyone and even
- enter it carefully, if someone is sitting near you.
- Never meet up with anyone you befriend online.
- Never open the emails \ attachments \ links coming from any unknown person.
- Be careful while sharing your photos on social media or with anyone.
- Never try to login as someone else and read their emails or access other data.

KEY POINTS FOR ONLINE CLASSES

- Parents/Students/Guardians must not share class invites/ links with anyone who is not a part of the school or class or has not been invited by the teacher.
- Parents/Students/Guardians must not take photos, screenshots, record videos/
- audios of the virtual sessions.
- All material shared on Google Classroom or Meet is the School's intellectual property and downloading/ circulating/ sharing of content without permission is strictly prohibited.
- Staff, parents and students must keep their identity safe and not share google passwords or their identity with anyone. Staff, parents and students must ensure they sign out of each session completely after completion of the session.
- Social media apps such as Snap Chat, Instagram, WhatsApp, or Facebook are not official, School-sanctioned channels of communication and must not be used for teaching and learning.
- Parents/Students/Guardians should inform the Teacher/School formally, in case a student is not able to attend any session.
- All users are required to be polite, respectful, and appropriate in their communications and must represent the school's values in their interactions with others, this applies for written words and as well as tone of conversation.
- The users(staff/students) must respect copyright and licensing laws with respect to software, information and other materials retrieved from the Internet.
- Users must not indulge in cyber bullying and writing of unkind remarks on the walls of unsuspecting friends, sharing of pornographic material through social media and/or email.
- The hacking and attempts at hacking the School personnel's email accounts, network and any other school assets have been and will continue to be dealt with the necessary seriousness.
- Report about abusive or illegal content or online bullying immediately to teacher or parents.
- Don't use other's information to login and not even attempt to infect or in way to tryto make someone else computer\device\credentials.
- Using the secured & encrypted SSL-VPN for remote access.

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 or communication devices in an offence.

TYPES OF ELECTRONIC CRIMES (E-CRIME)

- 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.
- 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.
- Cyber bullying: content may be offensive in a non-specific way, harassment directing 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 as Cyber bullying.
- Threats: Advertisements promising unrealistic products/services (adware) and software that intentionally causes harm (Malware)
- 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.

IT DEVICES/RESOURCES:

They include (such as desktops, notebooks, and tablets), storage devices (USB and flash memory devices, CDs, DVDs, floppy disks, iPod, 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 electronic and storage technologies

KNOW ABOUT CYBER BULLYING

To define bullying the most acceptable definition of cyberbullying which has been used is "an aggressive, intentional act or behaviour that is carried out by a group or an individual, using electronic forms of contact, repeatedly and over-time against a victim who cannot easily defend him or herself."

When the bullying happens online with the help of technology it is cyberbullying. Cyberbullying in India includes sharing private or personal information about someone which can cause embarrassment to the person.

PLACE OF OCCURRENCE OF CYBERBULLYING ARE AS FOLLOWS:

- Social Media (Facebook, Instagram, Snapchat, Twitter, etc.)
- SMS (text messages from the cellular network)
- Instant Message Services (WhatsApp, Facebook messenger, I message, etc.)
- Email

CYBERBULLYING FORMS AND EXAMPLES:

- Humiliating/embarrassing content posted online about the victim of online bullying,
- Hacking of account
- Posting vulgar messages
- Threatening the victim to commit an act of violence
- Stalking
- Child pornography or threats of child pornography

PARENT AND STUDENTS ACKNOWLEDGMENT:

- 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 copy of the agreement and policy for reference.
- 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.
- 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/ portal.
- The policy is available for download from the school website.

ACTION IN CASE OF SECURITY BREACH BY STUDENT

If any student breaches this policy, then he\she will be subjected to terms and conditions under Bal Bharati Public School Code of conduct Policy. And the case will be handled by the school inhouse "Cyber Cell" – a committee of 03 members – VP\HM of the school, 01 person from technical team (probably the tech. council member) & 01 person from class reps.

- 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.
- Major breaches (like cyber bullying, identity theft etc.) of this policy will result in the suspension period of up to ten weeks.
- 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.
- 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.
- 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.

- These actions may be taken even if the alleged incident occurs off site and/or out of school hours.

UNDERSTAND THE CYBER LAW

Section 2 (1) (nb) of Information and technology Act 2000

cyber security‖ means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction;]

Section 2 (1) (0) of Information and technology Act 2000

"data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

Section 2 (1) (r) of Information and technology Act 2000

"electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device; (s) "Electronic Gazette" means the Section 2 (1) (t) of Information and technology Act 2000.

"Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

Section 2 (1) (v) of Information and technology Act 2000

"Information" includes data, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche

Section 43 of Information and technology Act 2000,

If any person without permission of the owner or any other person Penalty for who is incharge of a computer, computer system or computer damage to network,— computer,

computer system, (a) accesses or secures access to such computer, computer system etc. or computer network; (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; (e) disrupts or causes disruption of any computer, computer system or computer network; (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder; (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.

He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. Explanation.—For the purposes of this section,— (i) "computer contaminant" means any set of computer instructions that are designed— (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network; (ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network; (iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource. (iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

(a) Section 471 of the Indian Penal Code, 1860 deals with whoever fraudulently or dishonestly uses as genuine any [document or electronic record] which he knows or has reason to believe to be a forged [document or electronic record], shall be punished in the same manner as if he had forged such [document or electronic record].

(b) Section 66A of the IT Act deals with any person who sends, by means of a computer resource or a communication device, –any information that is grossly offensive or has menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine Section 66C of the Information and Technology Act, 2000 Act deals punishment for identity theft and says that whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

(c) Sec 66D of the Information and Technology Act, 2000deals with punishment for cheating by personation by using computer resource, with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

(d) Section 66E of the Information and Technology Act, 2000 - whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

(e) Section 67 the Information and Technology Act, 2000: Punishment for publishing or transmitting obscene material in electronic form. Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

(f) Section 67A of the Information and Technology Act, 2000- Punishment for publishing or transmitting material containing sexually explicit act, etc., in electronic form. - Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

(g) Section 67B of the Information and Technology Act, 2000 deals with whoever, – publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children In obscene or indecent or sexually explicit manner; or cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or facilitates abusing children online, or records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

GOVERNANCE OF LAW

The BBPS Staff and students shall be abided by the school Cyber Policy and shall be governed by cyber security laws prevalent at the time being in force in the territories and states of India.

ACKNOWLEDGEMENT

I have read and been informed about the Cyber Security Policy of Bal Bharati Public School. I have received a copy of the policy and agree to abide by the policy guidelines as a condition of my employment in the school.

I understand that if I have questions, at any time, regarding the policy, I will consult with my immediate supervisor or IT department.

I have read the policy carefully to ensure that I understand the policy before signing this document.

Employee\Student Signature:

Employee Printed Name:

Receipt By:

Date:

Asha Prabhakar
(Principal)

Kindness, Resilience, Respect

Distribution:

Staff (via e-mail)
VPL, HMs, Academic Coordinator
Website (For perusal of parents)