المدرسة الهندية العالمية الخاصة
INTERNATIONAL INDIAN SCHOOL
P.O. BOX 5665, AJMAN, U.A.E | T : +971 67408333 | info@iisajman.org | www.iisajman.org

CYBER SAFETY AND SECURITY POLICY

Academic Year 2020-21
Reviewed & Updated : Term 2, September 2020

Abstract: This document lays down the school Cyber Safety policy on use of online mechanisms and platforms especially in the context of Online Learning. The intention is to make students and parents aware of the best practices and safeguards while using online platforms and make them aware about good online behavior and provide a reliable reporting mechanism in cases a student faces online issues.

Introduction:

Internet, the most interactive technological platform of this century, has become an integral part of our daily lives. It is a learning and communication tool that offers us a wide range of opportunities. It is an invaluable source of knowledge and encourages creativity and imagination. Internet ethics involves our approach while using it for different purposes. We should be aware that we should always be honest and respect the rights and property of others on the web.

Cyber safety refers to the safe and responsible use of information and communication technology. It is not just about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and using good 'netiquette' (internet etiquette). This policy covers all aspects of the technology usage of students with reference to school context both inside the school premises and in case of Online Learning too. The cyber safety and security policy is interlinked with the School Behavior Management Policy, Health and Safety Policy, Child Protection Policy and IT policy.

As per Article 21 of the UAE Federal Decree Law 5/2012, such cybercrimes like eavesdropping, interception, invasion of privacy, use of offensive language are punishable by extensive jail terms and heavy fines as well.

The school has a strong child protection policy , and the online safety and security violations will be considered and dealt as per the Wadeemas' law , Federal Law No. 3 of 2016, Issued on 08/03/2016. The law details the scope of the responsibility of the competent authorities and institutions, including the state to ensure care and protection of children. Protecting the child's right to life, staying alive and developing, having all necessary opportunities and to enjoy a free, secured and developed life, protecting the child from any form of negligence, exploitation and maltreatment and from any physical and psychological violence, protecting the child best interest, educating the child of his rights and duties and commitments.

Objectives:

- To enable the students to browse the internet safely and understand the importance of using secure connections.
- Inform the students and parents on the protective and safety measures in their use of technology, to be aware of Cyber Bullying
- To improve awareness of intelligent usage of social media websites and smart usage of educational websites.
- To communicate the etiquettes of electronic communication.

Scope of the Policy:

The policy is applicable from KG to Grade 12.

The DO's in the use of Online Technology and Electronic Communication:

- Respect the privacy of others.
- Report and flag content that is abusive or illegal.
- Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.
- Report online bullying immediately to the teacher and parents/ or someone whom you trust.
- Use a strong and unique password with combinations of numbers, uppercase and lowercase letter and special characters for each account(s).
- Keep the browser, operating system and antivirus up-to-date.
- Obtain software from trusted sources. Always scan files before opening them.
- Lock your screen when you finish using your computer/ tablet/ phone. Further, set it to lock automatically when it goes to sleep.
- Check to see if the web address begins with https:// whenever you sign in online.
- Make privacy settings in social media accounts in such a way that profile and posts are visible only to close friends and acquaintances.
- Connect only with known individuals.
- Be mindful of your digital reputation - think twice before you post something embarrassing, harmful or inappropriate.
- Report to the service provider immediately if the account is hacked. If possible deactivate your account.

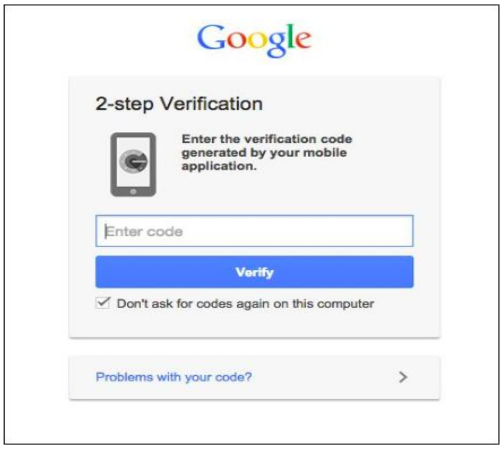
The DONT's in the use of Technology and Electronic Communication:

- Don’t share your mobile number or parent’s mobile number.
- Don’t share your address/location.
- Don't share your personal information: real name, date of birth, etc. unnecessarily.
- Don’t share bank account numbers or credit card numbers of your parents.
- Don’t share your Social Security number /Emirates ID.
- Don’t share your Passwords.
- Don't send your pictures to unknown persons or share them on social media.
- Don't open emails and attachments from strangers.
- Donˈ t respond to any suspicious email, instant message or web page asking for personal information.
- Don't enter a password when someone is sitting beside you as they may see it.
- Don't save your username and password on the browser.
- Don't steal otherˈ s information.
- Donˈ t access or use files without the permission of the owner.
- Don't copy software which has copyright without the authorˈ s permission.
- Don't bully others online by teasing, threatening, using rude or offensive language, making derogatory or hateful comments.
- Don't use someone elseˈ s password even if it is shared with you.
- Don't log in as someone else to read their emails or mess with their online profiles.

- Don't attempt to infect or in any way try to make someone else' s computer unusable.
- Don' t meet unknown (even if they are known only through online interaction) people alone; always inform your parent.
- Don't open or download any attachments from an unknown source as they may contain viruses.

Tips for safe internet browsing

1. Update your browser frequently
2. Turn on Two-Factor Authentication whenever possible. Most of the websites critical to our lives (online banking websites, Gmail, Facebook etc.) offer two-factor authentication.

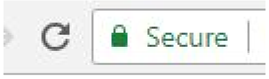


2-step Verification

Enter the verification code generated by your mobile application.

3. Customize your security settings. You can also make a browser more secure by customizing it through its preferences or settings menu.

4. Confirming site’s security (https vs http) Check for the Secure as shown on the address bar (Chrome).



5. Backup your data. This means finding a way to copy your information to a safe place so that you don’t rely on your computer’s hard disk alone.

6. Avoid clicking on links if possible from messages or chats. Viruses spread easily through links in instant messages and email attachments.

7. Bookmark important sites
   If there are sites you visit regularly, it’s a good idea to bookmark them in your browser. Bookmarked addresses take you to the same site every time.

Cyber Safety Challenges - Related Terms

- **Cybercrimes** are offences that may be committed against individuals, companies or institutions by using computers, internet or mobile technology. Cybercriminals use platforms such as social networking sites, emails, chat rooms, pirated software, websites, etc., to attack victims. Children are also vulnerable to various types of cybercrimes.
- **Cyber Grooming** is growing as one of the major cyber threats faced by children and teenagers. It is a practice where someone builds an emotional bond with children through social media or messaging platforms with an objective of gaining their trust for sexually abusing or exploiting them. The cyber groomers can use gaming websites, social media, email, chat rooms, instant messaging, etc. by creating a fake account and pretending to be a child or having the same interests as of the child.
- **Cyber bullying** means using internet or mobile technology to intentionally harass or bully someone by sending rude, mean or hurtful messages, comments and images/videos. A cyber bully can use text messages, emails, social media platforms, web pages, chat rooms, etc. to bully others.

The school has no tolerance for incidents of Cyberbullying and will take actions as per the national guidelines and laws in case such incidents occur and are reported.

Consequences of Cyberbullying

It can lead to both civil and criminal cases.

CIVIL LAWS

- Defamation.
- Invasion of privacy/public disclosure of a private fact.
- Intentional infliction of emotional distress.

CRIMINAL LAWS

Criminal laws can lead to the arrest and offenders can be put in jail and get fines as well. Using the internet for the following purposes will attract criminal cases in many countries.

- Hate or bias crimes.
- Making violent threats to people or their property.
- Engaging in coercion. Trying to force someone to do something they don't want to do.
- Making harassing telephone calls, sending obscene text messages, and stalking.
- Sexual exploitation and sending sexual images of children under 18 years of age.
- Taking a photo of someone in a place where privacy is expected (locker room, bathroom, etc.) and exploiting it on the internet.
- Taking a photo of someone without their consent and posting publicly.

If you feel that you are being Cyber Bullied

- Ignore.
- Tell someone.

- Just let a trusted adult know what's going on. The worst thing you can do is to keep it to yourself. Remember, it's not your fault!
- Do not instigate.
- If someone is sending you hurtful messages or posting mean pictures, they're doing it to get an emotional response from you. Don't give them one! Don't respond OR retaliate. This will only encourage them to take it further.
- Block them. If it's on Facebook or another website that allows you to block the person or leave the chat room, then do it!
- Be open to parents about your online identity and image.
- Tell your parents what you do online in general.
- Never indulge in cyber bullying yourself.

How Can I Use Cyber Platforms Safely?

- Follow the cyber safety guidelines properly.
- Safeguard your device and online accounts.
- Don't involve in any kind of improper cyber behavior, even for fun.
- If you face any challenge online, immediately inform your parent or elders so that they can support you and contact school if needed.
- Always maintain cyber etiquettes while using technology.
- Make a note that cybercrimes are punishable offenses; especially the UAE has very strict and stringent laws to deal with Cyber offences.

REPORTING

If a student faces an uncomfortable situation online, specifically if someone is threatening or bullying online, especially during Online Learning sessions, who should be contacted?

! Share with your parents or elders in family

! Students/Parents can write an email to the school counsellor.

Mr. Shamjith, Counsellor: counsellor.boys@iisajman.org

Ms. Mary Samna, Counsellor: marys@iisajman.org

! Students and parents can escalate the issue with Child Protection Officer(CPO) Principal / Child Protection Members : respective supervisors.

The numbers & email IDs are given as below.

Name: **Ms. Qurat Ul- Ain**, CPO Contact : 0558403796, email: principal@iisajman.org

Name : **Mr. Jayakrishnan**, Boys Section Contact : 0563548083, email: boyssection@iisajman.org

Name : **Ms. Hilda Mary**, Girls Section Contact : 0563547912, email:girlssection@iisajman.org

Name: **Ms. Rekha Sukumar**, Primary 2 Contact : 0563547884, email: primary2@iisajman.org

Name : **Ms. Jagrita Mazumdar**, Primary 1 Contact: 0563547882, email: primary1@iisajman.org

Name: **Ms. Saima** , KG Contact : 0563547870, email: kgsection@iisajman.org