المدرسة الهندية العامة العليا – راس الخيمة
INDIAN PUBLIC HIGH SCHOOL, RAK

(Recognized by the Ministry of Education, UAE, affiliated to CBSE, New Delhi)
Tel: 07-223124, Fax: 07-2222807, e-mail: iphs@eim.ae, www.iphsrak.com
P.O.Box: 5079, Ras Al Khaimah, UAE

عـــام زايـــد
YEAR OF ZAYED

CYBER SAFETY POLICY

2018-2019

VISION

To be a pioneer in education to produce students of noble mind.

MISSION

To serve as a model, where teaching and learning is innovative and to excel beyond the classroom.

MOTTO

Wisdom is better than riches.

CORE VALUES

Tolerance
Honesty
Respect
Responsibility
Generosity
Innovation

1. CYBER SAFETY POLICY

Purpose

- To develop and maintain rigorous and effective cyber safety practices with ICT devices while minimizing and managing any risks.
- To maintain a cyber safe school environment and also address the needs of students and other members of the school community.

STRATEGIES FOR CYBER-SAFETY

1. Only using the computers and other ICT equipment for learning.
2. Only going online or using the Internet at school when a teacher gives permission and an adult is present.
3. Always asking a teacher first if unsure whether allowed to do something involving ICT.
4. Only using their own username and not allowing anyone else to use that user name.
5. Keeping all passwords private.
6. Only using the Internet, e-mail, mobile phones or any ICT equipment for positive purposes. Not being mean, rude or offensive, or to bullying, harassing, or in any way harming anyone else, or the school itself, even if it is meant as a joke.
7. While at school:
   - Attempting to search for things online that are known to be acceptable at school. This excludes anything that is rude or violent or uses unacceptable language such as swearing and
   - reporting any attempt to get around, or bypass, security, monitoring and filtering that is in place at the school.
8. Following these steps if anything is found that is upsetting, is mean or rude, or that is known to be unacceptable at school:
   - not showing or sharing with others,
   - turning off the screen, and
   - getting a teacher straight away.
9. Only bringing ICT equipment/devices to school with written permission from home and the school. This includes things like mobile phones, iPods, games, cameras, and USB/portable drives.

10. Only connecting an ICT device to school ICT technologies, or running software (e.g. USB/portable drive, camera or phone) with written permission from the teacher. This includes all wireless/Bluetooth technologies.
11. Only using charging devices that have been electrically tested and certified by the school.
12. Complying with the school cyber-safety strategies for any ICTs brought to school.
13. Only downloading or copying files such as music, videos, games or programs with the permission of a teacher
14. Always asking a teacher's permission before putting personal information online, which includes any of the following:

    - full name
    - address
    - e-mail address
    - phone numbers
    - photos.

15. Respecting and treating all school lCT equipment/devices with care, including:
    - not intentionally disrupting the smooth running of any school ICT systems
    - not attempting to hack or gain unauthorised access to any system
    - following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICTs
    - reporting any breakages/damage to a teacher straight away.

Steps we take to protect students

- Use of a filtered service
- Supervision
- Planned activities
- Websites are previewed by teachers to ensure they are suitable for student's curriculum needs
- Teachers will choose the search engine
- Students are taught to use the internet safely

Safety points for students

- Only use your login username and password
- Do not delete files or settings
- Ask permission before using the internet or a website
- Only send approved emails
- Do not give you names or address to anyone online
- Do not enter chat rooms
- Ask permission before taking anybody's photo
- If you see anything you do not like report it to your teacher
- If you are bullied don't ignore the bullying tell someone you trust, never reply, ask a teacher for help

Cyber Bullying

Cyber bullying is bullying through the use of communication technology like

- mobile phone text messages
- e-mails
- websites
- social media

This can take many forms for example:

- Sending threatening or abusive/insulting comments through text messages, photos or e-mails, personally or anonymously
- Making insulting comments about someone for example on a website, social networking site.

Some of the more common types of bullying are:

- Text messages
- Pictures/videos via mobile phone cameras
- Chat room bullying
- Mobile phone calls
- Emails
- Bullying via websites

***Information for Parents*:** At **IPHS**, we take this form of bullying seriously and will deal with each situation individually.

Breaches of the policy

If students do not follow cyber-safety practices, the school may inform parents/caregivers, and in serious cases, may take disciplinary action against the student(s). Families may also be charged for any damage or repair costs where applicable.

…….