SCHOLARS
INDIAN SCHOOL

CYBER-SAFETY POLICY

In the wake of the Covid-19 Pandemic, Scholars Indian Private School requests all our parents and students to study the cyber safety guidelines for the effective progress of the distance learning. We have taken all the technological precautions in the school

- Ensuring that they keep their credential facility private and wont share with others.
- Reminding them that the chat messages will be visible to school staff and they are not supposed to send inappropriate messages in communication platforms (MS Teams, class WhatsApp group, Orison parent portal).
- Guiding them to follow an online conduct.
- Teaching them to do online assessments independently reinforcing school guidelines.

Safety Considerations:

- Don't put unnecessary personal information in the user profile of these apps. For example, try to keep location, phone number and dates of birth private.
- Always check the terms and conditions of the programs.
- Helping to educate the child on how to use these programs to ensure they are safe.
- Reminding the child to never accept instant messages, phone calls, screen sharing or files from someone they don't know.
- Providing the students school administered accounts and not to share their credentials with others.
- Educating the students on Cyber bullying, inappropriate content, ransom ware, over sharing and online predation.
- Sending an RUP (Responsible use Policies) to outline the responsible terms and consequence of misuse.
- Giving a Digital Citizenship Curriculum (privacy, security, relationship, communication, information, literacy and copyright).
- Providing resources (videos, blogs) to raise awareness to be safe online.
- Educating children to recognize potential internet threat.
- Awareness to students to consult the Resource officer if they are a victim of an online threat (Principal, Class teacher and IT Head)
- Setting up a planning team to address Cyber threat and to support student's emotional needs.
- Keeping the anti-virus program updated daily and allowing it to stay current. There are new attacks every day and the amount of malicious content on web applications is rapidly increasing in both frequency and expertise so it's important to stay up to date.
- If you have a wireless router, check that your wireless network is secure so that people living nearby can't access it.
- If your network is secure, users will be prompted for a password when they try to access it for the first time and there should be a padlock symbol next to the network name.
- Protecting them from the threat of online harm due to unsupervised and unfiltered screen time.

Technical Security

School will be responsible for ensuring that the school infrastructure and network is as safe as secure as possible.

- Servers, wireless systems and cablings are securely located and physical access restricted to authorised personnels only.
- School website is protected with SSL certificates (Https:\\) and all data are protected. Nobody can copy or download any content or files from the school website.
- The computers and servers are well installed updated with antivirus (ESET Nod 32) with parental control.
- Teaching and e-learning network is well maintained with firewall and admin network is installed with sonic wall router with Firewall.
- Removable devices are not permitted in the computer lab and classrooms as they are the source of spreading virus and threats between devices.
- Social media and unwanted websites are blocked in firewall by filtering mechanism inside the school teaching and learning network.
- All staff, students using the school devices (Computer lab, classroom) are submitting the acceptable use policy issued by the school.
- IT Coordinator is responsible for ensuring that software/Antivirus are accurate and upto date and is regularly checked.
- Appropriate security measures are in place to protect school system and data. School backups are well maintained and regularly transferred and saved in different locations of external storages.
- All online safety complaints are monitored and can be informed through an electronic monitoring system which is available in the school website.
- All users can easily access the incident reporting form available in the school website.
- All computers in the lab and classroom are configured with onscreen messages to alert about e-safety.
- Installation of any kind of third-party software is not allowed in the school computer devices.
- e-safety posters are screen saved as wall papers as a reminder on e-safety guidelines.

Cyber Safety Updated

- Avoiding video conferences that require students to create accounts.
- Protecting audio video recordings.
- Protecting student data privacy.
- Avoid sending emails to staff, students and parents that contain links.
- Never ask log in credentials via email.
- Implementing two-factor or multi-factor authentication.
- Privacy for teachers and students of turning on a webcam in a private home.

Safe Cyber Practices

- Saving the details of the students (name, class, division, devices, IP address and log in time)
- Fire wall protection for Network.
- Unwanted websites blocked in school system according to use.
- Separate user id for students in computer lab.

- Data controlled by parental control system.

Also refer:

Data Protection Policy
Reward and Sanction Policy
Anti Bullying Policy
Child Protection Policy

Adopted: April, 2020 **Reviewed and updated: March, 2022**

Hameed Ali Yahya K. M.
Principal