**SHARJAH INDIAN SCHOOL**
Tel: 06 5670560 / Tel: 06 5671866
Fax: 06 5672914 / Fax: 06 5675166
P.O. Box – 2324, Sharjah
e-mail: mail@sissharjah.com Website: www.sissharjah.com

**OUR VISION**
Educate Enlighten Empower

# CYBER SECURITY POLICY

# CYBERSECURITY POLICY

## 1.Policy brief & purpose

Having sufficient cybersecurity protocols is vital for schools systems as lack of cybersecurity can lead to exposure of confidential information and significant monetary loss. School maintain sensitive data on students, and it is critical to keep the information as secure as possible. We are committed to defend critical services with best-in-class cybersecurity solutions against unauthorized disclosure and theft of student records,hacks affecting school operation ,misuse and corruption of school technology.

## 2.Scope

This policy applies to all our staff, students, who has permanent or temporary access to our systems and hardware.

➢ **Protect personal data and devices**.

When staff use their digital devices to access trust emails or accounts, they introduce security risk to our data. We advise our staff /students to keep both their personal devices secure. They can do this if they:

- Keep all devices password protected.
- Ensure antivirus software is kept up to date.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into school accounts and systems through secure and private networks only.

➢ **Keep emails safe.**

Emails often host phishing attacks, scams or malicious software (e.g., trojans and worms) .To avoid virus infection or data theft, we instruct staff/students to

avoid opening attachments and clicking on links when the content is not adequately explained. If an employee/student isn't sure that an email they received is safe, they should contact their local IT Team.

- **Transfer data securely**

  Transferring data introduces security risk.Following measures are adopted

  - Avoid transferring sensitive data to other devices or accounts unless absolutely necessary.
  - Share confidential data over the private network/ system and not over public Wi-Fi.
  - Ensure that the recipients of the data are properly authorised people
  - Report scams, privacy breaches and hacking attempts.

- **Additional measures**

  To reduce the likelihood of security breaches, we also instruct our employees to:

  - Turn off their screens and lock their devices when leaving their desks.
  - Report stolen or damaged equipment as soon as possible IT support.
  - Change all account passwords at once when a device is stolen.
  - Report a perceived threat or possible security weakness
  - Refrain from downloading suspicious, unauthorised or illegal software.
  - Avoid accessing suspicious website.

- Network and data monitoring can identify malicious activity if properly managed; this area is covered by a combination of technology and IT administrators.
- Regular vulnerability scanning is done and help prevent exploits on documented vulnerabilities.
- Network segmentation -IT support system designate systems for private and regulated data. Lower priority activities are assigned to a designated area in the network to support student and staff personal devices and data.
- A policy with standards for passwords, including multi-factor-authentication (for google classroom and zoom)and enforcement mechanisms ensure hackers against unauthorized access.
- Trained IT staff monitor the network continuously and review alerts issued by manufacturers