

CYBER SAFETY POLICY

Our Vision

Empowering students with values and skills to excel in a dynamic world.

Our Mission

To deliver high-quality, forward-thinking education that equips every student with the knowledge, skills, attitudes and global competencies to excel.

To create a nurturing, inclusive environment where all learners are enabled to contribute meaningfully to their communities and beyond.

To inspire a passion for discovery, nurture innovative mindsets.

To develop individuals to embrace every learning experience, build emotional and mental fortitude and a growth mindset to navigate challenges confidently.

1. Intent

Sabari Indian School Dubai has a Statutory obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community,

These responsibilities are increasingly being linked to the use of the Internet and Information Communication Technologies (ICT), and a number of related cyber safety issues. The Internet and ICT devices/equipment bring great benefits to the teaching and learning programmes, and to the effective operation of the school.

Sabari Indian School, Dubai places a high priority on providing the school with Internet Facilities and ICT devices / equipment which will benefit student learning outcomes and the effective operation of the school.

However, the School recognizes that the presence in the learning environment of these technologies (some provided partly or wholly by the School and some privately owned by staff, students and other members of the school community), can also facilitate anti – Social, inappropriate, and even illegal, material and activities. The School has the dual responsibility to maximize the benefits of these technologies, while at the same time to minimize and manage the risks.

This policy intends to provide guidelines to ensure rigorous and effective school cyber safety practices.

2. Scope

Sabari Indian School, Dubai will develop and maintain rigorous and effective Cyber Safety practices which aim to maximize the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school. Whilst minimizing and managing any risks.

3. Definitions

These Cyber Safety practices will aim to not only maintain a Cyber Safety School environment, but also aim to address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

Important terms used in this document:

1. The abbreviation 'ICT' in this document refers to the term 'information and communication Technologies'
2. 'Cyber Safety' refers to the safe and responsible use of the Internet and ICT equipment /devices, including mobile phones
3. 'School ICT' refers to the school's computer network, Internet access facilities computers, other School ICT equipment/devices outlined below
4. The term 'ICT equipment/devices' used in this document, includes but is not limited to Computers (such as desktops, laptops, PDAs), storage devices (Such as USB and flash memory devices, CDs, DVDs, floppy disks, ipods, MP3 players), cameras (Such as video, digital, webcams), all types of mobile phones, video and audio players /receivers (Such as portable CD and DVD players), Gaming Consoles and any other similar technologies as they come into use.

4. Guidelines

Associated issues the school will address include: the need for on-going funding for Cyber Safety practices through inclusion in the annual budget, the review of the School's annual and strategic plan, the deployment of staff, professional development and training, implications for the design and delivery of the curriculum, the need for relevant education about Cyber Safety for the school community, disciplinary responses appropriate for breaches of Cyber Safety, the availability of appropriate pastoral support, and potential employment issues.

To develop a cyber safe school environment the school delegates to the Principal the responsibility to achieve this goal by developing and implementing the appropriate management procedures, practices, electronic systems and educational programmes.

1. No student may use the school Internet facilities and school-owned/leased ICT devices/equipment in any circumstances unless the appropriate use agreement has been signed and returned to the school. Use agreements also apply to the use of privately owned/leased ICT devices/equipment on the school site, or at / for any school-related activity, regardless of its location. This includes off-site access to the school network from school or privately-owned/leased equipment.

2. Sabari Indian School, Dubai user agreements will cover all employees, all students (including adult and community), and any other individuals authorized to make use of the school internet facilities and ICT devices/equipment, such as all teachers/staff, external, tutors and providers, contractors and other special visitors to the school.

3. Use of the internet and the ICT devices/equipment by staff, students and other approved users at Sabari Indian School, Dubai is to be limited to educational, professional development and personal use appropriate in the school environment as defined in individual user agreements.

4. The School has the right to monitor, access and review all use. This includes personal emails sent and received on the School's computers and network facilities at all times.

5. The School has the right to audit at any time any material on equipment that is owned or leased by the school, The School may also request permission to audit privately owned ICT devices/ equipment used on the school site or at any school related activity.

6. Issues relating to confidentiality, such as sighting student or staff information, reasons for collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of the school.

7. The safety of students is of paramount concern. Any apparent breach of Cyber Safety will be taken seriously. The response to individual incidents will follow the Procedures developed as part of the school's Cyber Safety practices. In serious incidents, advice will be sought from an appropriate source, such as a lawyer with specialist knowledge in this area.

There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may be reported to the relevant law enforcement agency.

8. In regard to any matter whereby the school believes there may be material which is of a bullying, sexual, racial or violent nature or where the school or students of the school may be brought into disrepute, the school reserves the right to permit specified staff to inspect any school – owned or personal devices brought onto school property, including but not limited to: Cameras, Video recorders, Computers, Mobile Phones or Mobile Phone Apps.

This inspection may also extend to Social Networking sites that are not Privately listed e.g facebook and Instagram.

Reviewed on 30th March 2025

Next Review on 30th March 2026



Clara Martin

School Principal