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 programmers, 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, as needed, 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.

The purpose of this policy is to establish guidelines for creating a safe online environment within our school community, promoting responsible digital citizenship and ensuring the well-being of all members.

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 s 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

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 programs.

All members of the school community must adhere to acceptable online behavior. Cyberbullying, harassment, discrimination, and any illegal activities are strictly prohibited.

Respect for others' privacy and intellectual property rights is paramount.

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, students), 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 and professional development 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 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.
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 professionals, lawyers 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.

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 s 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, tabs, iPads, 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.

5. Internet Usage

School-provided internet and devices must be used for educational purposes only.
Accessing inappropriate content, including explicit material, hate speech, Violent content, cyber-bullying, scams, malicious software, plagiarism and cheating, gaming and

entertainment personal use, inappropriate communication, copyright infringement.

6. Social Media Guidelines:

Social media platforms must be used responsibly, both within and outside of school hours.
Responsible sharing and interaction online are encouraged.

Prohibited Actions for Students:

- Cyberbullying or harassing others online.
- Posting or sharing inappropriate, offensive, or discriminatory content.
- Engaging in or sharing explicit content.
- Using social media during class time or school hours without permission.
- Sharing confidential or proprietary information, pictures, data about the school or its students/staff.
- Using social media to publicly criticize or defame the school or its administration

Prohibited Actions for Staff:

- Engaging in inappropriate communication with students on social media platforms.
- Sharing confidential information about students, colleagues, or the school without permission.
- Using social media during instructional time or for personal use during working hours.
- Posting content that could be interpreted as unprofessional or detrimental to the reputation of the school or its stakeholders.

Prohibited Actions for Parents:

- Engaging in cyberbullying or harassing behavior towards school staff, students, or other parents.
- Sharing confidential information about school policies, decisions, or individuals without permission.
- Using social media to publicly criticize or defame the school or its administration.
- Sharing photos or information about other students or school events without permission from their parents or guardians.

7. Data Protection and Privacy

The school's cyber safety policy prioritizes data protection and privacy by collecting and storing personal data with consent and only for necessary educational and administrative purposes. Access to personal data is restricted to authorized personnel, and appropriate security measures are in place to prevent unauthorized access or disclosure. Personal data is retained only for as long as necessary and securely disposed of when no longer needed. Student privacy is ensured, with parental consent obtained for data processing

activities, and procedures are in place to respond to data breaches effectively. Compliance with data protection regulations is regularly reviewed and overseen by an appointed Data Protection Officer or responsible staff member, ensuring the school maintains trust and confidence within the community.
Data will be shared with parents or registered guardians only, as needed.
Sharing personal information online without consent is prohibited.

8. Cyberbullying Prevention and Intervention

Cyberbullying is defined as the use of electronic communication platforms, such as social media, instant messaging, or email, to harass, intimidate, or harm others. It often involves repeated and deliberate aggressive behavior, such as spreading rumors, posting hurtful messages or images, or impersonating someone online, with the intention of causing emotional distress or embarrassment to the victim. Cyberbullying can occur anonymously and may have serious consequences for the mental health and well-being of the targeted individual.
Any cases of cyber bullying the incident must be reported to :

Class teacher → Assistant Principal → Child protection officer → Head of pastoral care → Principal.

9.Sanctions for Misuse

- Warning and Education: For minor or first-time offenses, students, staff, or parents may receive a warning about their behavior and be provided with educational resources on proper cyber safety practices.

- Parental Notification: In cases involving students, parents or guardians may be notified of the misconduct, and a discussion may be held to address the issue and collaborate on a resolution.

- Loss of Privileges: Individuals who misuse school-provided technology resources or violate cyber safety policies may face consequences such as temporary or permanent loss of access to school networks, devices, or online platforms.

- Disciplinary Actions: Depending on the severity of the offense, disciplinary actions may be taken, including detention, suspension, or expulsion for students, and reprimands or termination for staff members.

- Restitution: In cases where misuse of technology resources results in damage or harm to others, the responsible party may be required to make restitution, such as covering repair costs or providing compensation for damages.

- Legal Consequences: Serious violations of cyber safety policies, such as cyberbullying, harassment, or illegal activities, may result in involvement of law enforcement authorities and legal consequences, including fines or criminal charges.

- Counseling and Support Services: Individuals who are targeted by cyberbullying or

who engage in inappropriate online behavior may be referred to counseling or support services to address underlying issues and promote positive behavior.

- Training and Awareness Programs: The school may implement training programs or awareness campaigns to educate students, staff, and parents about cyber safety best practices and the potential consequences of misuse of technology resources.

10. Parental Involvement

Parents are encouraged to actively participate in their child's online activities. The school will not hold responsibility for online/digital activity of the students outside of school hours.

Resources for parents to educate themselves on cyber safety and support their children are: UAE Cyber Security Council, e-safety Campaign by UAE Government. Child Helpline (116111).

https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

This policy is designed to create a safer online environment within our school community, fostering responsible digital citizenship and promoting positive online interactions.

Reviewed on 01 April 2026

Clara Martin
School Principal

Sabari Indian School