ICT Acceptable Use 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. Introduction

Technology plays a pivotal role in education. At Sabari Indian School, we are committed to harnessing technological advancements to enhance learning while ensuring that all users engage responsibly, ethically, and in alignment with the Knowledge and Human Development Authority (KHDA) guidelines.

2. Purpose

This policy aims to:

- Define acceptable and unacceptable uses of digital devices and internet services within the school.
- Safeguard students, staff, and the school's digital infrastructure.
- Promote a secure, respectful, and productive digital environment.

3. Scope

This policy applies to all members of the school community, including students, staff, parents, and visitors, who access the school's digital resources or bring personal devices onto school premises.

4. Responsible Use Guidelines

4.1. General Use

- **Educational Purpose**: All technology use should primarily support educational objectives. Personal activities that do not align with this purpose are discouraged during school hours.
- **Compliance**: Users must adhere to all applicable UAE laws, KHDA regulations, and school policies when utilizing digital resources.
- Digital devices to be used during lessons only at the explicit discretion of teachers and only for as long as necessary to support educational objectives
- The school reserves the rights to implementing robust supervision protocols to protect students from inappropriate content, cyber threats, and other potential risks. Where permitted, the use of mobile phones other digital devises by students will be closely supervised.
- Students are required to hand in their phones or other devices with network/SIMs.

4.2. Network Usage

- **Access Control**: Users are granted access to specific network resources based on their roles. Unauthorized access or attempts to breach network security are strictly prohibited.
- **Bandwidth Management**: Activities consuming excessive bandwidth, such as streaming non-educational content or downloading large files without permission, are not allowed.

4.3. Social Media

- **Professionalism**: When representing the school online, users should maintain professionalism. This includes using appropriate language, sharing accurate information, and refraining from engaging in disputes or negative discussions.

- **Privacy**: Users should adjust privacy settings to protect personal information and be cautious about the content they share, ensuring it does not harm the school's reputation or the safety of its community members.

5. Ethical Code

5.1. Ethical Code for Students

5.1.1. Academic Integrity

- **Plagiarism Prevention**: Students must ensure that all assignments, projects, and research work are their own. Proper citation of sources, whether from books, websites, or other digital materials, is required.
- **AI and Digital Tools**: The use of artificial intelligence (AI) and other digital tools must align with ethical academic practices. Students should not rely on AI-generated content unless permitted by their teachers.
- **Cheating and Misrepresentation**: Copying from peers, using unauthorized resources during assessments, and falsifying data in research projects are considered academic misconduct.
- **Proper Citation Methods**: Students should familiarize themselves with citation styles and referencing and apply them correctly in their work.
- **Use of Digital Platforms for Learning**: Online research must be conducted responsibly, ensuring that sources are credible, accurate, and relevant to the subject matter.

5.1.2. Digital Etiquette

- **Respectful Communication**: Students should use polite and appropriate language when engaging in online discussions, emails, and group chats related to school activities.
- **Responsible Social Media Use**: Students should refrain from posting inappropriate, offensive, or harmful content on social media that could negatively impact themselves, their peers, or the school's reputation.
- **Cyberbullying and Online Harassment**: Any form of cyberbullying, including spreading false information, making derogatory comments, or engaging in harmful online behavior, is strictly prohibited.

- **Privacy and Confidentiality**: Students should respect the privacy of others and avoid sharing personal details, passwords, or sensitive school-related information online.
- **Email and Messaging Conduct**: When communicating via email or school-approved messaging platforms, students should use professional language, include clear subject lines, and avoid excessive use of emojis or informal slang in formal communications.
- **Appropriate Use of Digital Resources**: School-provided digital resources, including learning management systems, online libraries, and shared folders, should be used solely for academic purposes. Accessing or sharing unauthorized files, games, or unrelated materials is not allowed.
- **Participation in Online Classes and Forums**: When attending virtual classes or discussion forums, students should follow the school's netiquette guidelines, including muting their microphones when not speaking, dressing appropriately, and maintaining a distraction-free environment.

5.2. Teachers

- **Role Modeling**: Teachers should exemplify ethical digital behavior, guiding students in proper technology use.
- **Continuous Learning**: Educators are encouraged to stay updated on emerging technologies and integrate relevant tools to enhance the learning experience.

5.3. Parents

- **Partnership**: Parents should collaborate with the school to reinforce responsible technology use at home, ensuring consistency with the school's policies.
- **Monitoring**: Regular discussions about online activities and monitoring of digital device usage can help children navigate the digital world safely.

6. Digital Use Ethics

6.1. Responsible Use of Technology

- **Use for Educational Purposes**: All digital devices, including computers, tablets, and mobile phones, should be used primarily for educational and school-related

activities. Personal use during school hours should be limited and aligned with school policies.

- **Accessing Approved Content**: Students and staff must only visit websites and use applications that are deemed appropriate by the school. Unauthorized access to restricted content, including explicit, violent, or illegal material, is strictly prohibited.
- **Fair and Equal Access**: School resources, such as shared computers, projectors, and internet access, should be used fairly and efficiently. Users must not monopolize devices or bandwidth by downloading large files unrelated to schoolwork.

6.2. Privacy and Security

- **Personal Information Protection**: Users must not share their personal details (such as full names, addresses, phone numbers, or passwords) on public platforms.
- **Confidentiality of School Data**: Students, teachers, and staff must maintain the confidentiality of sensitive school-related information, including exam papers, student records, school documents and staff communications.
- **Use of Secure Passwords**: All digital accounts must be secured with strong passwords. Passwords should not be shared, and users should update them regularly.
- **Multi-Factor Authentication**: If provided, users should enable multi-factor authentication (MFA) for additional security on school platforms.
- **Protection Against Cyber Threats**: Users must avoid clicking on suspicious links, downloading unverified files, or engaging in activities that could introduce viruses or malware into the school network.

6.3. Ethical Online Communication

- **Respectful Digital Interactions**: Users should engage in polite and constructive communication across all digital platforms, including emails, school forums, and social media.
- **No Harassment or Cyberbullying**: Harassment, hate speech, and cyberbullying (including spreading false information, posting harmful comments, or sharing private content without consent) will result in serious disciplinary action.

- **Appropriate Social Media Use**: Students and staff should represent the school positively online. Posting defamatory, offensive, or misleading information about the school or its members is strictly prohibited.
- **Email Etiquette**: Users should write clear and respectful emails, avoiding unnecessary informal language, excessive use of capital letters, or inappropriate attachments.

6.4. Digital Footprint and Online Reputation

- **Awareness of Digital Permanence**: Users must understand that online actions leave a permanent digital footprint. Content posted online can be retrieved and misused even after deletion.
- **Responsible Content Sharing**: Users should think critically before sharing images, videos, or comments online. Content that may harm personal or school reputations should not be posted.
- **Avoiding Misinformation**: Students and staff must verify sources before sharing information. Fake news, propaganda, and misleading content should not be circulated.

6.5. Ethical Use of Digital Resources

- **Copyright and Intellectual Property**:
    - Users must respect copyright laws and give proper credit to sources when using digital content.
    - Plagiarism (copying text, images, videos, or software without permission) is strictly prohibited.
    - Students must use citations and references in academic work when using external sources.
- **Software Licensing and Usage**:
    - Only authorized and licensed software should be installed on school devices.
    - Downloading, sharing, or using pirated software is illegal and against school policy.
    -

- **Ethical Use of AI and Online Tools**:
    - AI-based tools (such as ChatGPT, Grammarly, or Google Translate) must be used ethically and in accordance with school guidelines.
    - AI should not be used to generate assignments or replace original student work.

6.6. School Network and Internet Usage

- **School Network Access**:
    - The school's internet and Wi-Fi should only be used for educational purposes.
    - Unauthorized access, hacking, or attempting to bypass security filters is strictly forbidden.
- **Bandwidth Management**:
    - Streaming non-educational videos, downloading large files, or engaging in excessive gaming on the school network is not permitted.
    - Teachers and staff have priority access to bandwidth-intensive applications required for lessons.
- **Monitoring and Compliance**:
    - The school reserves the right to monitor network activity to ensure compliance with the Acceptable Use Policy.
    - Any attempt to alter network settings or disrupt school IT systems will lead to disciplinary action.

6.7. Digital Ethics for Teachers and Staff

- **Professional Conduct**: Teachers must uphold high standards of professionalism in digital communication and use of online resources.
- **Student Data Protection**: Teachers must ensure the confidentiality of student records and academic data.
- **Online Classroom Management**: Teachers should use digital platforms to create a safe and engaging learning environment, ensuring respectful discussions and appropriate content sharing.

- **Use of Personal Devices**: Staff should avoid using personal devices for school-related work unless authorized by the administration.

6.8. Consequences of Digital Misuse (Ref.Behaviour Policy)

- **Minor Violations** (e.g., inappropriate website access, excessive personal device use):
    - Verbal warning and counseling.
    - Temporary restriction from school devices or internet access.
- **Moderate Violations** (e.g., disrespectful online behavior, unauthorized social media posts, academic dishonesty):
    - Written warning and parental notification.
    - Loss of access to school networks or platforms for a specified period.
- **Severe Violations** (e.g., cyberbullying, hacking, data breaches, sharing explicit or harmful content):
    - Suspension or expulsion as per KHDA regulations.
    - Legal action if the offense violates UAE cyber laws.

7. Mobile Phone Usage

Reflecting KHDA's emphasis on minimizing distractions and promoting effective learning environments, Sabari Indian School has established the following mobile phone guidelines:

- **Student Use**: Students are required to keep mobile phones switched off and stored in designated areas during school hours, including breaks and extracurricular activities, unless a teacher grants explicit permission for educational purposes.
- **Staff Use**: Teachers and staff should limit personal mobile phone use during instructional time and ensure that their usage does not interfere with professional responsibilities.
- **Parental Communication**: Parents are encouraged to contact the school's main office for urgent matters rather than contacting their children directly during school hours.

Mobile Phone Regulations

- Student Mobile Phone Use:
- The use of mobile phones by students is strictly prohibited during school hours.
- Students using own transport (Grades 6–8 only) may bring mobile phones to school, but they must immediately hand them over to their class teacher upon arrival.
- If siblings are involved, only the oldest sibling will be allowed to carry the mobile phone, provided parental consent has been obtained from the school.
- All students who carry their phones must have a prior approved consent form from school with parents signature.
- Unauthorized Mobile Phones:
- Students who are not permitted to carry mobile phones but are found with one will have it confiscated immediately.
- The phone will only be returned after a meeting with the parents.
- If any other student has a valid reason to bring a mobile phone to school, parents must email the class teacher a day in advance for approval.
- Teacher Mobile Phone Use:
- Teachers are not allowed to use mobile phones during lessons, supervision duties, or any other assigned responsibilities.
- Teachers must not use mobile phones during classes under any circumstances. Their use of mobile phones within the school premises should be strictly limited and regulated. If a teacher is found using a mobile phone excessively or during lessons, strict action will be taken.
- Teachers must not bring student phones into the classroom.
- Teachers must register the contact details of their spouse or a designated family member with the school reception.
- In case of an emergency, their family members may contact the school reception, and the school will assist in communication as needed.
- Communication with Parents:

- Parents or family members must register at the school reception if they need to meet a student.
- In case of an emergency, families can contact the school directly.

8. Network and Device Security

8.1. Passwords

- **Creation**: Passwords must be a minimum of eight characters, incorporating a mix of letters, numbers, and special characters to enhance security.
- **Confidentiality**: Sharing passwords is prohibited. Users should log out from devices after use to prevent unauthorized access.

8.2. School Devices

- **Usage**: School-owned devices are to be used strictly for educational activities. Personal use is discouraged and may be subject to monitoring.
- **Maintenance**: Users should not attempt to repair or modify school devices. Any technical issues or damage must be reported to the IT department promptly.

9. Consequences of Misuse

Violations of this policy can lead to:

- **Privilege Revocation**: Temporary or permanent suspension of access to specific or all digital resources.
- **Disciplinary Measures**: Actions may range from verbal warnings to suspension or expulsion, depending on the severity of the violation.
- **Legal Implications**: Engaging in illegal activities, such as hacking or distributing pirated software, will result in legal action in accordance with UAE cybercrime laws.
- KHDA takes abusive conduct seriously and enforces a zero-tolerance policy for any misuse of mobile phones by students, staff, governors, or visitors that could be deemed criminal or culturally insensitive. Such incidents will be promptly reported to the relevant authorities to ensure appropriate action is taken.

10. Review and Monitoring

This policy will be reviewed annually or as required to ensure its effectiveness and relevance.

Effective Date	March 1, 2025
Policy Review Date	March 1, 2026

Mrs. Clara Martin

Principal
Sabari Indian School