ONLINE SAFETY POLICY

INTRODUCTION

Scholars Indian Private School e-Safety policy is developed to maintain rigorous and effective e-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, while minimizing and managing any risks. These e-Safety practices aim to not only maintain a cyber safe 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.

OBJECTIVES

The purpose of this policy is to

- Disseminate the principles of online safety to all the stake holders of the school.
- To safeguard staff and students of the school from cyber related issues and to light a path of joyful and safe learning experiences.
- To help students and staff to monitor their own standards and practice.
- To have clear structures to deal with online bullying.
- To ensure that all members of the school community are aware of unacceptable online behaviours and the retributions in case of violation of the norms.
- To instil in students a strong sense of responsibilities of a digital citizenship.

RISK ASSESSMENTS

- Exposure to inappropriate online content.
- Visit to hate / extremist sites
- All forms of online bullying
- Identity theft
- Sharing passwords and disclosure of personal information.
- Health and wellbeing (no. of hours spend on surfing ,social media and gaming)
- Sexting
- Copy right for intellectual property and ownership.
- Excessive use which may impact the social and emotional development as well as the learning of the students .

Dissemination/Communication of the Policy:

This policy is made accessible, communicated, and understood by all stakeholders through various ways such as:

- School website
- School portal
- Scholars App
- Hardcopy of policies maintained in the school.
- Soft copy sent through email.
- Display on notice boards
- Policy is made as a part of annual induction pack for new and returning staffs and students.
- Stated in the Acceptable Use Policies (AUPs) for students, parents, staff, visitors, community uses.

- Through general and department meetings and also through training conducted by e - Safety officer .

ONLINE SAFETY OFFICER: Hameed Ali Yahya K M(Principal)

Mobile No.: 00971-56-2915459

ONLINE SAFETY GROUP

1. Mr. Habib Ur Rahman (Chairman)
2. Mr. Hameed Ali Yahya K M (Principal)
3. Mrs. Syamala Prasad (Administrator)
4. Ms. Preetha M (Vice Principal)
5. Mr. Prasad (Academic Advisor)
6. Mrs. Bitty Devasia (School Counsellor)
7. Mrs. Ambili Shaji (Health & Wellness Coordinator)
8. Mrs. Jeena (Team leader grade 1-4)
9. Mr. Shemeer (IT Coordinator)
10. Mrs. Sameeha (HoD of Computer Department)
11. PTC president
12. PTC secretary
13. Student Representative 1
14. Student Representative 2
15. Student Representative 3
16. Mr. Shihas (Community Advisor)
17. Mr. Avinash (Community Advisor)

ROLES AND RESPONSIBILITIES

School Management

- To be responsible for the approval of the e-Safety and for reviewing the effectiveness of the policy through the annual reports, incident log and monitoring and auditing reports submitted by the e-Safety Group validated and confirmed by the Senior Leadership Team.
- To ensure that appropriate funding is authorized for any e-Safety solutions, relevant training to all staff and other activities as recommended by the Senior Leadership Team.
- To be actively involved in promoting e-Safety information to parents and the wider community
- School management will extend the monetary support and approvals to update the infrastructure for maintaining a safe cyber environment and learning across the school community.

PRINCIPAL

- To foster a culture of safeguarding where e-Safety is fully integrated into whole school safeguarding
- To ensure that policies and procedures are followed by all staff
- To implement the procedures to be followed in case of a serious e-Safety allegation being made against a member of the school community
- To ensure that the e-Safety officer and group members receive proper training to enable them to carry-out their e-Safety roles effectively and to train other staff

- To support the e-Safety group in the implementation of the eSafety Policy and in their monitoring role
- To ensure that the Governing Board are regularly updated on the nature and effectiveness of the e-Safety
- To ensure that there is a system in place to monitor and support the ICT Managers who carry out internal technical online safety procedures
- To liaise with the safeguarding leads on all online-safety issues which might arise and receive regular updates about school issues and broader policy and practice information
- To take overall responsibility for data management and information security ensuring that the School follows best practices in handling information
- To ensure that child protection is the priority to be considered in sharing data information
- To ensure that the school implements the effective use of appropriate ICT systems and services such as filtering, technical security, protected email system, cloud system in accordance with child-safety principle

ONLINE SAFETY OFFICER (PRINCIPAL)

- To develop an e-Safe culture throughout the school community as part of safeguarding, this is in line with national best practice recommendations.
- To take overall responsibility for online safety provision.
- To take the overall responsibility for data and data security
- To ensure that school uses approved online security mechanism which is aligned with UAE cyber security law and policies of school.
- To be responsible for ensuring that staff, students and parents are receiving suitable awareness and training.
- To be aware of procedures to be followed in the event of a serious e – safety incident.
- To regularly monitor the online grievances and to ensure that the timely action is taken.
- To ensure that the Online safety incident log is kept up to date.
- Receiving complaints and disseminating to the concerned.
- Conducting meetings for online safety group and the whole school.
- To ensure that the appropriate action is taken upon the receiving of the concerns.
- To organise training to the online safety group and the whole school.
- To support the school by encouraging parents and the wider community to be active in e safe activities
- To report the cases to external body in case not able to solve by the school
- To audit and evaluate current practice to identify strengths and areas for improvement in collaboration with e-Safety Group Members
- To ensure that e-Safety is promoted to parents/or guardians and the wider community through a variety of channels and approaches-such as professional development workshops, sharing circular and policy updates.
- To liaise with the IT coordinator in ensuring that filtering is in place, which is actively and regularly monitored.
- To collaborate with the IT team for data protection and data security and specific related policies to ensure that practice is in line with legislation.
- To maintain an e-Safety incident/action log to record incidents and actions taken.
- To liaise with the local entity such as MOE and or other local and national bodies as appropriate.
- To report regularly to Senior Leadership Team.

- To ensure that all staff is aware of the procedures that needs to be followed in the event of an Online Safety incident.

VICE PRINCIPAL

- To ensure that there is an age and ability appropriate e-Safety curriculum that is embedded, progressive, flexible, and relevant which engages children's' interest and promotes their ability to use technology responsibly and to keep themselves and others safe online.
- To establish /review online related policies.
- To ensure that any incident of cyber bullying is logged, and appropriate measures and sanctions have been taken in line with Anti-bullying Policy, Student Behaviour Policy and Discipline Policy.

IT COORDINATOR – Mr. Shemeer(Mobile No.: 00971-55-4894352)

- To ensure that the school follows all current online safety advice to keep the children and staff safe.
- To support the school by encouraging parents and the wider community and engage in e-safety activities.
- To keep up-to-date documentation of the school's online security and technical procedures.
- To ensure that all data related to students are adequately protected.
- To ensure that all network services are managed on behalf of the school.
- To ensure that the whole school abides by the password policy
- To confirm that the whole school has undergone multifactor authentication.
- To guarantee the perfect functioning of filtering system.
- To ensure the user appropriate internet access.
- Regular audit of antivirus, Malware, back up and system recovery.
- To protect the personal data of stake holders and keep them informed on their rights and obligations.
- To receive reports of e-Safety incidents and keep a log of incidents for appropriate action, follow-up and future e-Safety development.
- To provide advice and e-Safety training for all stakeholders.
- To be responsible in blocking access to potentially dangerous sites to prevent the downloading of the dangerous files.
- To maintain an up-to-date documentation of e-Safety guidelines, protocols, and procedures, and ensure that all policies are communicated to all stakeholders and sign agreements are obtained.

PTC Members

- Awareness to parents on e-safety.
- Extending staunch support to school to bring to notice areas of improvements as parent representatives.
- To be an integral part in policy implementation and updating.

Student Members (School parliament representatives)

- Creating awareness on safety through videos, short films, posters and brochures among the school community.

- To conduct trainings for student community.
- To ensure that the policy is aligned with the need and requirements of students.

School counsellor

- Provide students with a comprehensive school counselling program that ensures equitable academic, social and emotional development opportunities for all students in physical learning and virtual learning.
- Cooperate with all relevant stakeholders, including students, educators and parents/guardians when student assistance is needed, including the identification of early warning signs of student distress.
- Facilitate short-term groups to address students' academic, career and/or social/emotional issues and inform parent/guardian(s) of student participation in a small group.
- Promote awareness of school counsellors' ethical standards and legal mandates regarding confidentiality and the appropriate rationale and procedures for disclosure of student data and information to school staff.
- Individual and group counselling of students regarding issues that might impact on their school adjustment.
- Presents timely topics and trends about the issues concerning school and children which will benefit the students, school staff and parents in physical and virtual learning.
- Emotional support and guidance to the staff who are in need of such.
- Physical Meeting / Virtual Meeting) with the parent/s in order to cater children's counselling needs during online and offline classes.
- Conducts Guidance Lessons to help children learn about social and emotional skills which are fundamental in their development and growth.
- Liaise with external agencies, service providers and other schools to ensure provision of maximum support to meet children's well-being.
- Educate students on how to participate in the virtual school, in order to minimize and prevent potential misunderstandings that could occur - perhaps, due to absence of visual and/or verbal cues that would otherwise provide additional contextual meaning to the school counselling process during regular face-to-face meetings.
- Incorporate lessons that align with academic, career and social/emotional domains.
- Report to parents/guardians and/or appropriate authorities when students disclose a perpetrated or a perceived threat to their physical or mental well-being.

Staff Representatives (Supervisors/ Team leaders)

- Promotes awareness and commitment to online safeguarding throughout the school community as per the requirements
- Takes responsibilities of online safety issues and contributes in reviewing the online safety policies and documents.
- To promote an awareness of online safety to all the members of the community and help them develop their commitment and support to the full implementation of e-Safety Policy
- To regularly update e-safety issues and legislation and be aware of the potential risk for serious child protection issues.
- To oversee the delivery of the online safety element linked with curriculum.
- To supervise and guide students carefully when engaged in learning activities involving online technology.

- To ensure that the digital communications with pupils should be on a professional level and only through school-based systems.

COMMUNITY ADVISORS

- Read and understand the policy and support the school with proper updates.
- Help school in conducting trainings.
- Update school IT infrastructure like software, school portal and school portal and school website to ensure the online safety and security.
- Help to develop organize and implement events.
- Maintain availability and approachability to respond to online safety needs and issues.

ALL STAFF

- Understand and comply with the policy.
- To have an understanding on whom to contact and how the procedures of reporting and action works.
- Sign the acceptable use policy and understand the sanctions in case of violations.
- Encourage students to strictly follow the online safety etiquettes.
- To link curriculum with e safety activities
- Take a zero-tolerance approach towards cyber bullying and that of other forms.
- Staff can only use the school provided Microsoft outlook email system.
- Non-teaching staff shall have a thorough understanding of the policy and put utmost care in safeguarding the students in corridor, bus, playground and restrooms.

ROLE OF STUDENTS

- To be a responsible user of the school digital technology systems in accordance with their signed agreement of the Student Acceptable Use Policy (AUP) and other related eSafety policies and guidelines
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- To ensure that communications with other students, staff members and members of outside community do not harass, vilify, or attack personally other individuals. This includes, but is not limited to, written words and the posting of images.
- To understand the importance of reporting abuse, consequences of misuse and access to inappropriate materials.
- To know and understand all policies of school.
- To understand the importance of adopting good online safety practice when using digital technologies out of the school.
- To take the responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To know how to report the concerns and be aware of the designated officer to report.
- To spread the word of safety with the community.

ROLE OF PARENTS

- To ensure that their children understand the need to use the internet, mobile devices, and any other technology in an appropriate way.
- To take the opportunity to attend e-Safety training conducted by the school, parent's meeting for any e-Safety information and issues
- Read, understand and sign the online safety policy document.
- To support the school in promoting online safety and endorse the students Acceptable Use Agreement which includes the pupils use of the internet.
- To encourage children to follow the Acceptable Use Agreement..
- To access the school website / Learning Platform in accordance with the relevant school Acceptable Use Agreement.
- To consult with the school if they have any concerns about their children's use of technology.

EDUCATION:

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- e -Safety Induction at the beginning of the school year for all staff and students.
- A planned e-Safety curriculum that is an integral part of the ICT, Digital Citizenship, and other lessons and that should be regularly reassessed.
- Key e-Safety messages are reinforced in various subject lessons, assemblies, webinars, and other school activities.
- Students are constantly reminded to be critically vigilant of the materials/ content that they access online. Likewise, they are guided to validate the accuracy of the information.
- Students are taught to acknowledge and to respect copyright of the source of information/materials used on the internet.
- Students are helped to understand the terms and conditions in the Student Acceptable Use Policy (AUP).
- Staffs are continuously trained to make them role models of good e-Safety practices and develop digital resilience.
- Parents will continuously be provided of e-Safety training and information campaign through webinars, newsletter, website, email, WhatsApp to enhance a deeper awareness of the e-Safety practices to monitor and guide their children.
- The management is encouraged to initiate and/or participate in e-Safety training/awareness session to enhance their understanding about e-Safety practices
- Online safety and etiquettes are incorporated in curriculum subjects like ICT, Science, Social, Moral Education, Mathematics and languages incorporate the need and importance of online safety.
- Students are given access to only the age appropriate and content appropriate materials under the guidance of teachers during on campus classes.

e- Safety Prevention Duty of Care

All staff is encouraged to be vigilant and persistent in inculcating to the minds of the students the e-Safety best practices. As part of their pastoral care, they must ensure that students:

- Develop the courage to talk openly to their parents and/or guardians about what they see online and tell them if anyone asks for personal information
- Commit themselves to follow the e-Safety rules in school and family rules when playing online games.
- Understand the importance of being cautious when sharing personal information online that includes real name, address, phone number, school name, password, and other private information
- Commit to follow the following e-Safety ethics: Post only information or photo that you feel comfortable sharing with the whole world and Never use the ICT technology in spreading gossip, bully or hurt other's reputation and feelings
- Identify the security tools available on most computers/devices to protect their information and protect their devices from virus and malwares
- Enhance awareness about the online potential unreliable influences about their beliefs and ideas and report immediately the incident to a trusted adult in the school

MANAGING THE IT AND COMPUTING INFRASTRUCTURE

- The school has educational filtered secure broadband connectivity.
- Blocks all chartrooms and social networking sites except those that are part of an educational network or approved learning platform.
- Have strong password for all operating systems.
- The school is vigilant in supervision of pupils use at all times.
- Provides advice and information on reporting offensive materials.
- Ensures that all the staff and students have signed the Acceptable Use Policy.
- Never allow to conduct raw image search using search engines.
- The Online learning materials are carefully scrutinised before sharing with the students.

DETAILS OF IT INRASTRUCTURE IN SCHOOL-2021-2022

Sl.	Items	Quantity
1.	Smart Panels (Smart Board)	47
2.	Servers	2
3.	Desktop Computers	38
4.	Laptop Computers	4
5.	Televisions	11
6.	Projectors	5
7.	IP Telephone	15
8.	Printers	7
9.	Routers and access point	7
10.	Switches	6
11.	Network IP Camera (Hikvision)	41
12.	Webcam	55

School Website	:	www.rakscholars.com
School Parent Portal	:	www.orison.school
Router	:	Sonic Wall Router
Remote learning application	:	Microsoft office 365 (Microsoft Teams)
Antivirus	:	ESET Nod 32 antivirus and Windows firewall (Windows Defender)
Operating system	:	Windows 7, 8, 10 & 11.
Microsoft office	:	Office 2007, 2013 and 2016.
Softwares	:	Microsoft Teams (e-Learning Platform), Orison School (Mobile Application for School for education both Android & I-phone).

NETWORK MANAGEMENT

- Uses individual, audited credentials for all users.
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services.
- Uses administration system control tools for controlling.
- Ensures that the network manager is up to date.
- The computers which are allowed for the students have students login and they could access only limited sites
- Scans all portable devices with antivirus before it is connected to the network.
- Staff access to the school's management information system is controlled through a separate password for data security purposes.
- Insists all users to log off when they have finished working or are leaving the computer unattended.
- The smart boards in the class could be accessed by the students only under the supervision of teachers.
- All mails received by the school are scanned before opening it.
- Makes clear responsibilities for the daily back up of finance systems and other important files via server.
- Does not publish the email addresses of students and staff on the school website.
- The videos and the photos of the students are posted in the social media sites controlled by the school only after receiving the consent from the parents.
- Online learning Platform is perfectly secured; staff and students could login only using the credentials into the class groups added by the IT Governor.
- Maintains equipment to ensure health and safety.
- All computer equipment is installed professionally and meets health and safety standards.

SCHOOL WEBSITE

- The online safety officer takes the overall responsibility to ensure that the website content is accurate; updated and the quality of presentation is maintained.
- The information is uploaded only by the authorisers.

- The materials are mostly the information regarding the curricular and cross curricular activities, works and accolades of the students.
- The photographs and videos are published after taking the consent from the respective individuals or parents.

LEARNING PLATFORMS

- Uploading of information on the school's learning platform is shared between different staff members according to their responsibilities.
- All the uploads will be accessible to the members of that particular group.
- Students are allowed to upload only after the approval by the concerned teacher incharge.
- The videos uploaded to the school learning platform will be only accessible by members of school community.

SOCIAL NETWORKING

- School has an active Facebook page and Youtube account in which the activities of school are displayed.
- Comments under Facebook posts are regularly monitored and blocked in Youtube.
- Awareness on the use of social media is constantly given to students, staff and parents.
- Awareness on security settings on personal social media profiles are regularly given to minimise risk of loss of personal information.

CCTV

The CCTV provision is installed in the school to ensure the security of students, staff and visitors of the school. The recordings are kept confidential and will be shared with the concerned external department for any investigation.

LINK WITH OTHER POLICIES

The online safety policy is linked with

- Child protection policy
- Behaviour policy
- Induction policy
- Rewards and sanctions policy
- Anti-bullying policy
- Assessment policy
- SEND policy
- Digital Health and safety policy
- Parliament policy
- Social media policy
- Child protection policy

  All the above policies are shared to all the members of the school community through website for their perusal and to follow the modus operandi of the school.

MANAGING MOBILE TECHNOLOGIES

- The school allows staff to bring in personal mobile phones and devices for their own use. However the use of mobile devices in the classrooms that interrupts teaching or learning is not allowed.
- Personal devices cannot be connected to school's network.

- Students are not allowed to bring the mobile phones to school, the school may give a special permission in serious situation, if requested by the parents. The phone will be under the safe custody of the class teacher during the class hours. The name of the student will be indicated on the mobile and will be returned after the class.
- Students are given the consent by the school to carry the gadgets along with them during picnic or study tour. However the school will not take any responsibility for the damage or loss of the gadgets.
- Students who are bringing the mobile devices to school without seeking the permission of the school will have their devices confiscated and will be in the school's custody till the intervention of parents in this regard.
- Staff and students are not allowed to record the audio, video or capture the picture of anyone in the school until they are given the formal consent to do so.
- Teachers could record the activities of classroom with the prior consent of Principal.
- Staffs are allowed to use their mobile phones only for academic purpose during their free hours inside the staffroom.

Bring Your Own Device (BYOD) Policy

BYOD is a special privilege given to students of our school which allows students to bring their device and use their own devices for events like International exams, for digital events like Digital Fest Competitions, school Exhibition etc. Wireless access will be provided to students during the conducting of the event. Permission to bring and use personal devices is contingent upon adherence to responsible use guidelines. Please note that if a personal device is used by a student for malicious purposes, to contravene privacy or to cause disruption to the educational environment, student's network or Internet access privileges may be revoked or limited.

Definition of Personal Device

For purposes of BYOD, portable electronic hand-held device/equipment like laptop and tablet are only allowed that can be used for word processing, wireless internet access, image capture and recording, sound recording and the transmitting, sending and storage of information. Wearable technology timepieces (such as smart watches) and fitness bands are not permitted.

At Scholars, smartphone usage as BYOD is not permitted. BYOD is for use in classroom or event time only. Data (of any type) should not be uploaded to the Internet (or be stored/used in a publicly visible digital location) without the verbal permission of the teacher.

Conditions of Use

- All students may use a personal technology device in school network by completing and submitting the attached BYOD Policy agreement.
- The use of personal technology device is solely limited to supporting and enhancing educational situations. They are to be used with the guidance of teachers, in and around the classrooms. personal technology device should not be used for non-educational purposes in lessons unless the student is given permission to do so by the teacher.
- Only the school network can be accessed on campus by students.
- Students must respect their peers and staff at all times when using personal technology devices. No malicious usage is permitted. Students may not engage in any malicious behaviour involving the use of personal technology device or intend to cause disruption to the school network.

- Students may not record images (still or moving) of other students or members of staff without first gaining their personal permission to do so.
- Students should be aware that staff will be able to ask a student if they can view the contents of their personal technology device if there is reasonable suspicion that the student has violated the BYOD policy agreement, school rules or is engaged in any other misconduct when using the device in school.
- Students may not use a privately-owned personal technology device in lessons unless they have submitted a signed copy of this document to their teacher in advance.
- No student shall establish a wireless peer-to-peer network using his/her personal technology device, or any other wireless device, while in school.
- The teacher may request, at any time that personal technology device be turned off in the classroom or outside. Failure to do so may result in revocation of access to school network.
- Sound should be muted on all personal technology device during lesson or event unless the teacher authorises the use of sound.
- No student shall use another student's network login details and password.
- No school owned software may be installed on a personal technology device by a student.
- Students may not attempt to use software, utilities or other means to access internet sites or content that is blocked by the school's internet/network filters. Usage of VPN software is not allowed.
- Students must take full responsibility for their personal technology device at all times, unless the teacher gives permission for them to be stored in the classroom, in a secure location (eg: lockable filing cabinet). However, personal technology device would still be stored at the owner's risk.
- school will not provide a repair service or software installation to any personal technology device.
- This policy is in addition to acceptable use policy and agreements that are already in existence.

Lost or stolen devices

The user is entirely responsible for his/her own Personal Technology Device. The device should be treated responsibly and used with care. School will accept no responsibility for PTDs that are damaged, lost, stolen, or which have data infected/corrupted. Teachers will help students identify how to keep personal technology devices secure, but students have the final responsibility for securing their devices.

BYOD PARENT AND STUDENT AGREEMENT FORM

Student Name: _____ Grade: _____

I/we have read the SCHOLARS Bring Your Own Device (BYOD) RESPONSIBLE USE AND AGREEMENT FORM and hereby agree to the conditions of use as stated in it.

I/we understand that this policy form and the privilege to use personal technology device at SCHOLARS may be revoked at any time.

I/we understand that any violations of this policy may result in access to the school network being withdrawn when used in conjunction with a personal technology device.

I/we give permission for ……. (please print name) to use a personal technology device(s) on the school wireless network.

Device	Device Type, Brand and Model No	Virus software installed (if applicable?)
1		

Parent/guardian signature: …… Date: ……

Student signature: …… Date: ……

ACCEPTABLE USE AGREEMENT FOR STUDENTS

Scholars Indian Private School expects all the students to follow the following instructions for the secured and an effective learning in and outside the school.

- I will use only the school internet and other ICT facilities provided by the school under the supervision of staff.
- I will not attempt to download school technology.
- I will only access content suitable to my age.
- I will not access the file of other users. I will access the contents using my credentials only.
- I will create a strong password and change it on a regular basis.
- I will see that the flash drive which I bring to school is virus free and malware free and will not download any of the contents in the school system without the permission of the teachers.
- I will not upload or download contents that are offensive and illegal and will report to the teachers if in case I find something like that.
- I will not share the photo, video or any work of others without the consent of the school and individuals.
- I will avoid chat with strangers and will not use the school platform or system for any of my personal use.
- I will keep the browser, antivirus and operating system up to date in my system.
- I understand that all my use of internet in the school is regularly monitored and logged.
- I understand that all these rules are to ensure my safety and I will have to undergo sanctions on the violations of the same.
- I will not post any comment in the chat area of learning platform and will respect the identity of each individual.
- I will use only the school approved communication system to connect with my teachers and classmates for school related works.
- I will adhere to copyright restrictions while downloading the material from the internet.

ACCEPTABLE USE AGREEMENT STATEMENT FOR STAFF

- I will use school's digital technology resources for school's academic and professional purpose.
- I understand that the school will monitor my use of the school's digital technology and communication systems.
- I will keep my password of school technologies private.
- I will use strong passwords and keep changing it frequently.
- I will not browse, download or send material that could be considered against the protocol of country and school.
- If found any inappropriate or malicious content or file, I will inform the authorised IT personnel.

- I will not leave the device unlocked while not attending it.
- I will not access, copy, remove or otherwise alter any other user's files without their consent.
- I ensure that I will capture and publish the images of others only with their permission and in accordance with the school's policy.
- I will not allow unauthorised individuals to access mail, internet or other school systems using my credentials.
- I will ensure all documents are saved accessed and deleted in accordance with school's network security and confidentiality protocols.
- I will not connect any external device to the school network without the consent from authorised personnel.
- I will ensure that school data is transported from one location to another with permission of authorised authority of the school.
- I understand that failure to comply with this policy could lead to disciplinary action.
- I will not engage in any online activity that may compromise my professional responsibilities.

ACCEPTABLE USE AGREEMENT FOR VISITORS/PARENTS

Visitors who are seeking the permission to access school wifi will be given the permission only if the school finds it is to meet the emergency needs.

- I will abide by the rules of the school and will not access any inappropriate or illegal sites.
- I will decline the access once the work is done.
- I will not access any of the school devices.
- I am aware of the consequences on violating the school policies.

INDUCTION

- Every new staff and student is inducted on the online safety policy and the guidelines to be followed as a part of the Scholars Indian Private School.
- The staff and students have to sign the acceptable use guidelines at the time of joining to have an access to all the online systems of the school.
- All the access will be denied once they are not the part of the school

ASSET DISPOSAL

- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed through an authorised agency.
- Disposal of any equipment will conform to the waste management authority guidelines.

DEALING WITH COMPLAINTS

1. There is a form available in the school portal to address the concerns related to online safety (bullying) with the school. All parents are informed on this.
2. The complaint will be filed through the form which will be verified by the online safety officer.
3. The complaint will be then dispensed with the IT governor and reporting team to investigate and come back with findings.
4. After the interview with the complainant and the parent, they will be made aware of the actions that are to be followed.
5. The investigating officer, the Data protection officer will meet the complainant to gather further information.
6. The officer will track and investigate to get the clear picture of it.

7. The report will be provided to the online safety officer who will then communicate with the complainant in not more than 15 days.

APPENDIX

1. Password Policy
2. Data Protection Policy
3. Incident Report Form.
4. Grievances Policy
5. Social Media Policy
6. Cyber Safety Policy
7. Acceptable Use Policy
8. Guidelines for parents on cyber safety
9. Guidelines for teachers on cyber safety
10. Guidelines for students on cyber safety

Adopted: April, 2020 **Reviewed and updated: April, 2023**

Hameed Ali Yahya K M
Principal
e- Safety Officer