WISE INDIAN PRIVATE SCHOOL

King Faisal Street

Al Riqqah,

Umm Al Quwain

UAE

WISE INDIAN PRIVATE SCHOOL

POLICY NAME	**E-Safety Policy**	POLICY NO.	WISE/POL/HSE/
EFFECTIVE DATE	April 1, 2021	**DATE OF LAST REVISION** March, 2024	**VERSION NO.** 002

VERSION HISTORY					
VERSION	**AUTHOR**	**REVISION DATE**	**DESCRIPTION OF CHANGE**	**APPROVED By:**	**Signature of Approving Authority:**
001	**Kavitha Ashly** Admin Officer	April 1, 2021	New Policy Draft	**Sofiya Singh** Principal	
002	**Ambika M** Admin Officer	March 1, 2024	Policy Revision	**Anjana Iraddi** Principal	

DEFINITION:

E-safety means being safe on the internet and practicing judicious use of mobiles, tablets and social media.

AIM

This policy is part of a suite of e-safety documents and strategies developed:

- to protect and educate all stakeholders in their use of technology
- to educate all stakeholders to be aware of, and respond responsibly, to risks related to social media platforms,
- to have the appropriate mechanisms to intervene and support any incident where appropriate.

This policy includes guidelines for safe and responsible uses of
- Internet in school
- Social media by all stakeholders
- Messenger app

Purpose:

Wise Indian Private School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E-Safety policy covers the internet but it also covers mobile phones and other electronic communications technologies.

We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential.

This policy aims to be an aid in regulating ICT activity in school, and provides a good understanding of appropriate ICT usage that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

POLICY:

WISE UAQ

> **The cchool e-Safety Coordinator is** MS. Greeshma
>
> Signature: ....

Making use of ICT and Internet in School:

Internet refers to the Worldwide Web. **Electronic Devices** refer to any computer, notebook tablet or other mobile device which can link through Wi-Fi or internet cable to the internet.

PURPOSE:
- The purpose of this policy is to set forth policies and guidelines for access to the school computer system and acceptable and safe use of technology resources and the Internet.
- To ensure the appropriate use of information and communication technologies to support effective teaching and learning in the school by protecting students from exposure to harmful materials, communications, and conduct on the Internet through usage of a reliable system for filtering the Worldwide Web sites, and to inform the school's principal and teachers when students access or use inappropriate materials on the Internet, and prevent students from accessing immoral sites and other inappropriate sites.
- To prevent unlicensed persons from having access to the school details.

Responsible use of ICT and internet:
- *Do not share your password with anyone.*
  - Log out of your account and devices after use.

- *Do not share any personal information or other people's (home address, phone number etc.)*
- *Be wary of emails that ask for any personal information.*
- *Check with an adult about anything you see that concerns you or report it to a teacher.*
- *Never meet up with anyone offline that you have only met online without a parent or trusted adult.*
- *Think carefully about the places you go online and keep focussed when on learning tasks.*
- *Take good care of the ICT equipment.*
  - Copy / upload / publish / distribute materials that are appropriate.
  - Take images or video of other pupils, friends or staff only with their full knowledge and permission.
  - Do not copy / upload / publish / distribute images or videos of others without their permission.
  - Do not copy materials, music, videos or pictures from the internet and use them in your own work unless they are copyright free.

- Remember that anything you do can be traced back including your browsing history and content that you may copy / upload / publish or distribute.
- Wi-Fi is provided in designated areas of the school where the password is shared only with staff.
- Students are permitted to access internet in the computer lab, library and class room only under adult supervision.
- The school uses licensed antivirus and office software.
- The data is examined with the content security regarding their integrity. Content filtering technique is used to prevent or block users from viewing inappropriate or objectionable website.
- Periodic checks are done for all the computers to check appropriate use of each computer.
- In case students misusing the internet, warning letter will be issued to the students.

- *You must understand that if you are irresponsible in your use of ICT, you may lose your access to it.*

Learning to evaluate internet content

With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the *school e-safety coordinator.* Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

Managing information systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practically possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by *the IT technicians/ICT coordinator/network manager* and virus protection software will be updated regularly.

- ensuring that all personal data sent over the internet or taken off site is encrypted
- making sure that unapproved software is not downloaded to any school computers.

Alerts will be set up to warn users of this
- files held on the school network will be regularly checked for viruses
- the use of user logins and passwords to access the school network will be enforced
- portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

Emails

The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication.
Staff and pupils should be aware that school email accounts should only be used for school-related matters, ie for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. **The school has the right to monitor emails and their contents** *but will only do so if it feels there is reason to.*

School email accounts and appropriate use

Staff should be aware of the following when using email in school:
- Staff should only use official school-provided email accounts to communicate with pupils, parents or g u a r d i a n s . Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their supervisors or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.

Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class

- in school, pupils should only use school-approved email accounts
- excessive social emailing will be restricted
- pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails   either from within the school or from an external account. They should not attempt to deal with this themselves.
- pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Pupils will be educated *through the ICT curriculum* to identify spam, phishing and virus emails and attachments   that could cause harm to the school network or their personal account or wellbeing.

USE OF SYSTEM IS A PRIVILEGE, NOT A RIGHT

The use of the school computer system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the school system or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate school policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws.

UNACCEPTABLE USES OF SCHOOL INTERNET:

A. The following uses of the school computer system and Internet are considered unacceptable for students and staff

1. Users will not use the school system to access, review, upload, download, store, print, post, receive, transmit or distribute:
   - pornographic, obscene or sexually explicit material or other visual depictions that are harmful to minors;
   - obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;
   - materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;
   - information or materials that could cause damage or danger of disruption to the educational process;
   - materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.

2. Users will not use the school system to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

3. Users will not use the school system to engage in any illegal act or violate any local, state or federal statute or law.

4. Users will not use the school system to vandalize, damage or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the school system software, hardware or wiring or take any action to violate the school security system, and will not use the school system in such a way as to disrupt the use of the system by other users.

5. Users will not use the school system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.

6. Users will not use the school system to post private information about another person or to post, transmit or distribute personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.

7. Users must keep all account information and passwords on file with the designated school official. Users will not attempt to gain unauthorized access to the school system or any other system through the school system, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user. Messages and records on the school system may not be encrypted without the permission of appropriate school authorities.

8. Users will not use the school system to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.

9. Users will not use the school system for conducting business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the school. Users will not use the school system to offer or provide goods or services or for product advertisement. Users will not use the school system to purchase goods or services for personal use.

B. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school official. In the case of a school employee, the immediate disclosure shall be to the employee's immediate supervisor and/or the administrative officer. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy.

Published content and the school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only. **For information on the school policy on children's photographs on the school website please refer to section 7.2 of this policy.**

Role and responsibility:

The school website Coordinator is Ms. Greeshma   Signature: ....

WISE UAQ

Policy and guidance of safe use of children's photographs and work

Colour photographs and pupils work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/guardians will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to.

The school will ensure that

- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Pupils are encouraged to tell a staff member if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our **school child protection and safeguarding policy.**

Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our **complaints policy** for more

information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the school's **child protection and safeguarding** policy and **behaviour policy.**

Social networking, social media and personal publishing

Pupils are not allowed to access social media sites like personal publishing tools including blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes in school. There are various restrictions on the use of these sites in school that apply to both students and staff.

Mobile phones and personal device

Students are prohibited from carrying mobile phones at all times.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined below.

- Mobile phones can be confiscated by a member of staff in case the pupil is found carrying one, and the device can be searched by a member of the senior leadership team if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- The school will not tolerate cyberbullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the **School Behaviour Policy.**
- Mobile phones must be switched off during school lessons or any other formal school activities.
- The school will not take responsibility for personal devices that have been lost, stolen, or damaged.
- Images or files should not be sent between mobile phones in school.
- If staff wish to use these devices in class as part of a learning project, they must get permission from a member of the Senior Leadership Team.

Mobile phone or personal device misuse

Pupils
- Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile phone may be confiscated.
- Pupils are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.

WISE UAQ

Staff
- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.
- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the **child protection and safeguarding policy**, or in the staff contract of employment.

Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

A. WHATSAPP USAGE:
Class group chat:

- The class teacher will be the admin of the group.
- It is used for school and school related matters; not community posts.
- Messages are not sent after 7pm or before 6am.
- Issues or questions that apply to a single child only are sent via direct message to their parent.
- No need to respond to all messages posted on the group, especially if it's a 'thumbs-up' or 'smiley face', only if specific information is requested.
- The group should never be used as a platform to air views/grievances regarding a teacher, child or parent in the class or school.
- The group is not a political platform for airing opinions on current affairs.
- The group should not be used for private conversations with anyone else using the group.
- The class teacher reserves the right to remove any member from the group on the basis of rude or unacceptable behavior.

Responsible use of group chats by parents:

- These groups are intended as a convenient way to distribute important school information to parents quickly and efficiently and for parents to communicate easily with each other regarding class matters, e.g. homework.

- The group should never be used as a platform to air views/grievances regarding a teacher, child or parent in the class or school.
- The group is not a political platform for airing opinions on current affairs.
- The group should not be used for private conversations with anyone else using the group.

WISE UAQ

- The school has a Complaints Policy in place, kindly avoid broadcasting grievances on group chats
- Be sensitive towards the teachers' personal time. Do not message after 7:00 pm or before 6:00 am.
- Parents, please keep an eye on children's WhatsApp groups. These are wide open to cyberbullying and young children have not yet developed the tools to handle this. If you pay the cell phone bill, then you have every right to monitor their online presence.
- The school has a clear communication channel (outlined above) and no complaints/grievances may be communicated via the class group-chat.
- Breaches of this code of conduct will be taken seriously by the school and, in the event of illegal, defamatory, or discriminatory content, breaches could lead to prosecution.
-

B. PARENTAL USE OF SOCIAL MEDIA:

Appropriate use of social networking sites by parents

The school recognises that many parents and other family members will have personal social networking accounts which they might use to discuss/share views about school issues with friends and acquaintances.

However, it is not the way to raise concerns or complaints as the school will not respond to issues   raised on a social networking site. If there are serious allegations being made/concerns being raised,
social media or internet sites should not be used to name individuals and make abusive comments.
Please contact the school to discuss any concerns you may have.

Inappropriate use of social networking sites by parents

- Although social networking sites may appear to be the quickest and easiest way to express frustrations or concerns about the school and those associated with it, it is rarely appropriate to do so. Other channels such as a private and confidential discussion with Supervisors, the Principal or member of the Governing Body, or using the school's formal complaints process are much better suited to this. The school considers   the following examples to be inappropriate uses of social networking sites. (This list is non-exhaustive and intended to provide examples only):
- Naming children or posting any undesired comments about children who attend Wise Indian Private School;
- Making allegations about staff or anyone else connected with the school;
- Making any posts that could be deemed to be cyber-bullying;
- Making complaints about the school or staff at the social media sites
- Making defamatory statements about the school or staff at the school;
- Posting negative or offensive comments about staff or any other individual connected to the school;
- Posting racist comments;
- Posting comments which threaten violence;
- Posting comments or engaging in online discussions with children other than their own.

Parents should also ensure that their children are not using social networking and other internet sites in an inappropriate manner. It is expected that parents/carers explain to their children what is acceptable to post online. Parents/carers are also expected to monitor their children's online activity, including inrelation to their use of social media. Please note that most social networking sites require the user to be at least 14 years old.

Procedure the school will follow if inappropriate use continues

The school will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step the school will usually discuss the matter with the parent to try to resolve it and to ask that the relevant information be removed from the social networking site in question. If the   parent refuses to do this and continues to use social networking sites in a manner the school considers   inappropriate, the school will consider taking the following action:

- Take legal advice and/or legal action where the information posted is defamatory in any way or if the circumstances warrant this;
- Set out the school's concerns to the parent in writing, giving a warning and requesting that the material in question is removed;
- Contact the police where the school feels it appropriate – for example, if it considers a crime (such as harassment) has been committed or in cases where the posting has a racial element, is   considered to be grossly obscene, grossly offensive or is threatening violence;
- If the inappropriate comments have been made on a school website or online forum, the school may take action to block or restrict that individual's access to that website or forum;
- Contact the host/provider of the social networking site to complain about the content of the site and ask for removal of the information;
- Take other legal action against the individual following appropriate advice.

Protecting personal data

Wise Indian Private School believes that protecting the privacy of our staff and pupils and regulating their safety through   data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and   how it is used. National curriculum results, attendance and registration records, special educational needs   data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and   academic progression of our school body to ensure that we are doing all we can to support both staff and students.

The   school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, MOE, or the   Department of Health. These authorities are up-to-date with data protection law and have their own policies   relating to the protection of any data that they receive or collect.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.