Online Safety Policy- IPHS

POLICY OBJECTIVE

The Online Safety Policy provides an insight into the overall safety norms when technology is used in the different domains of the school. This policy is designed to demonstrate and implement good and safe digital practices for all staff, students and parents.

AIMS

This policy ensures that:

- Students can safely access new technology and learn how to participate in the digital world without compromising their safety and security.
- a planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- All students and staff understand the importance of password security and the need to log out of accounts.
- Staff act as good role models in their use of ICT, the Internet and mobile devices
- It has a clear and understood arrangements for the security, storage and transfer of personal data.
- to create awareness among the stakeholders on 'the various initiatives of U A E in relation to child protection by incorporating the Federal Law No: 3 of 2016 **(Wadeema's Law)-Federal Law No. 3 of 2016** concerning child rights, which states that all children must be provided with appropriate living standards, access to health services, education, equal opportunities in essential services facilities without any kind of discrimination, Federal Law No: 5 of 2012 on combatting cybercrimes –the article of this law highlights a number of computer and online related activities and how they would be dealt with under the law. It addresses subjects such as IT security, invasion of privacy, malicious and illegal activities including hacking, fraud, improper system use, defamation, threats to state security, terrorism, insult to religions, and many more etc.
- It will deal with incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / caregivers of incidents of inappropriate e-safety behaviour that take place out of school.

ROLES AND RESPONSIBILITIES

The designated Online Safety Leader shall take the responsibility for any online safety issues and concerns and will be leading the online safety group. There are certain roles and responsibilities laid down to ensure the implementation of this Policy (Refer-Schools Online Safety Group rules and responsibilities). Here are the responsibilities listed out for core members of the group.

Roles and Responsibilities of Senior Leaders (Principal and Parent Council Representative)

•Evaluate, support and monitor the entire e-safety procedures and program of the school.

•Ensure that the online safety leader and group knows their responsibilities and adheres to the same.

•Ensure that the e-safety drive of the school is in line with the school development plan.

•Attend the online safety group meetings as ex officio members at least once a month.

•Represent the school for seminars and meetings along with the online safety leader where the presence of the school leader(s) is deemed imperative.

Roles and Responsibilities of Online Safety Leader/E- Safety Officer

•Provide leadership to the e-safety initiative of the school.

•Develop an e-safety culture in the school through a varied range of initiatives such as events, trainings, workshops, curriculum, and soon.

•Receive necessary training in e-safety, child protection and related topics and keeps updated about the latest developments on the same.

•Ensure that all members of the online safety group know their responsibilities and carries them out diligently.

•Have scheduled meetings with the group to discuss and address e-safety needs of the school.

•Convene emergency meetings in case of any incidents that require immediate attention and action.

•Ensure that all meetings have proper minuting and the same is filed for future reference.

•See to it that all departments systematically document all required matters related to e-safety such that they are easily accessible.

•Work with the school management, Principal, and HR Department to understand, develop and impart continuous training to the staff on online safety, acceptable use, child safety, anti-bullying and all matters related to e-safety.

•Ensure that e-safety policies are properly executed, reviewed and updated.

•See to the embedding of e-safety threads across policies of the school where they are relevant and essential.

•Develop, implement and monitor reporting strategies and systems to ensure that all e-safety incidents happening in and beyond school are addressed and followed up in a proper manner.

•Ensure that the e-safety curriculum is developed, imparted and updated as per plans.

•Work with the school team to plan and execute events and activities throughout every school year to promote e-safety.

•Ensure that parents are informed and involved in the e-safety journey of the school.

•Liaise with government and non-government agencies to stay updated and also to report any incidents that require outside the school intervention/advice.

•Understand the statutory requirements of e-safety in UAE and ensure that the school systems are incompliance.

•Represent the school for seminars and meetings on e-safety.

•Do adequate research, connect with various organizations and communities so that all the latest development in e-safety is known, and the same is integrated into the school where relevant

Roles and Responsibilities of Online Safety Coordinator (IT Department)

•Ensure that the technical infrastructure is secure and is not open to misuse or malicious attack.
•See to it that the digital infrastructure meets required e-safety technical requirements and/or other relevant points from varied policies.
•Ensure that the school has proper age-appropriate filters in place, and these are monitored, reviewed and updated regularly.
•Take measures to ensure that users may only access the networks and devices through a properly enforced password and all such passwords are subject to change based on the requirements of the password policy of the school.

•Develop rubrics, structures and schedules for the monitoring, auditing and reviewing digital infrastructure and ensure that online safety leader and other relevant authorities are informed of any incidents or breaches.
•Ensure that all infrastructure related audits reports, incidents, breaches and the actions taken are properly documented,
•Stay connected to contracted and other agencies for digital infrastructural maintenance and the addressing of issues that cannot be solved from within the organization.
•Ensure that the online safety leader and group members are updated regarding any changes or improvements brought about in the system.
•Provide the online safety leader/school management /school leadership yearly reports on the digital infrastructure of the school.
•Be up to date with new developments with regard to digital infrastructure and e-safety so as to effectively advise the management and online safety group, update the systems and ensure there is no redundancy.

Roles and Responsibilities of Online Safety Assistant Coordinator (Staff representative)

•Work closely with the online safety leader in leading the committee and all roles and responsibilities.
•Follow upon the plans for the year and ensure that they are being carried out systematically.
•Advice the online safety leader of any deviations from plans or any breaches that need attention for the leader and the group.
•Guide the Student Online Safety Group (Student Council members) in their activities.

Roles and Responsibilities of Child Protection Officer

•Take the lead along with online safety leader in ensuring in child protection.
•Immediately respond or step in when an online child safety incident occurs and work with the online safety leader, parents and students as required to address the same.
•Ensure that the evidence of intervention is documented.
•If appropriate, advise Online Safety Leader and school leadership for referral to external agencies.
•Be a part of the development, implementation and reviewing of the child protection policies of the school.
•Actively participate in the development of training modules for stake holders on child protection, online behaviours and anti-bullying.
•Obtain training on handling various child protection and e-safety issues and stay updated on the same.

Educating IPHS Community

Educating School Leadership and Online Safety Group

Before the rest of the school community is made aware of the importance on online safety and safeguarding measures, it is essential for the school leadership as well as members of the Online Safety Group to be equipped. For this the school ensures that they obtain relevant training from outside accredited organizations as well as experts in the field on the same. The

school management shall also see to it that the leadership and the group attend webinars and conferences (as deemed relevant) to keep themselves updates and bring about improvements in IPHS's e-safety initiative.

Educating students and parents

Ensuring that students and parents are well aware of the online safety norms and all related policies is part of the mission of the IPHS e-safety initiative. For this the school embeds e-safety into its action plan **(reference ICT Action Plan)** and runs programs, events and workshops throughout the year. The programs have clearly set learning outcomes and built-in feedback and/or assessment systems that ensures that the outcomes are met with. In case there is a gap, follow up programs are done to bridge the same. Some initiatives to ensure awareness are:

•All relevant policies updated on the school's website.

•Induction program for parents and students on e-safety at the beginning of the academic year.

•Periodic posters, tips and articles sent to parents and students (age appropriate) on digital safety.

•Classroom activities and events that involve students so that they learn about e-safety hands on.

•In-corporating e-safety in other subjects where chapters enable the same.

•Introduce and run a PHSE curriculum that in-corporates strands of e-safety.

•Ensure that students are given due classes on digital citizenship.

•Distribution of updated student handbooks to both parents and students at the beginning of every academic year.

•The important helpline numbers provided on the website.

•Oath taken by students at the beginning of every year on e-safety

Acceptable usage agreement is signed by every parent on behalf of their wards when they join the school.

•Parents are explained the relevance of the Media Release Consent Form and they sign the same at the beginning of the academic year.

•Reminders sent to parents to read up and understand e-safety guidelines posted on website.

•Updates on policies and guidelines communicated to parents and students when such updates occur.

•Student council active involvement in educating their peers about e-safety

Educating Staff

Just like students and parents, it is very essential for all staff of IPHS to be aware of and be well equipped with online safety and all related policies. For this the following plans are put into action every year.

•Every new staff is inducted on e-safety norms.

•Refresher programs and workshops are provided to staff throughout the year at different pre-fixed intervals.

•Training on how to detector look for signs of abuse and the system of alerting the required persons in case of a suspected case.

•Every staff signs the Acceptable Use Agreement when they join the organization.

•Regular tips and updates are shared with staff on e-safety.

•The IT Department regularly send staff updates on how to increase the security of their system. They are also given alerts for antivirus update and password change.

•Awareness program is conducted regarding the school reporting systems for online incidents, child protection and other relevant areas as well as the sanctions connected with them. This helps them support each other, students and parents where needed.

Strategies for Managing Unacceptable Use

The school takes full responsibility for ensuring that the school digital infrastructure is safe and secure as is reasonably possible and that policies and procedures for ensuring e-safety are adhered to without fail. It shall also ensure that the relevant people named in the online safety group will be effective in carrying out their e-safety responsibilities. Other strategies that IPHS shall take up to curb unacceptable usage are as below:•

The firewalls and filtering systems are set in place and are monitored closely by the IT Coordinator.

•Student centered events, programs and activities shall be conducted throughout the year.

•Regular trainings, workshops, quizzes and sessions shall be conducted for staff, students and parents to increase the awareness on online safety and responsible way of using the technology.

•Regular audit of the filtering system shall be conducted by the IT coordinator and all the reports and findings are given to the online safety leader in the irregular online safety group meetings.

•School shall put into action the set sanctions for both staff and students for managing the unacceptable use of technology and all the actions are taken in accordance with the guide lines provided in the MoE student behavior policy.

•IT coordinator shall ensure that only school provided credentials are only used for logging into the school network and other school digital platforms.

•Clear reporting system shall be in place so that online incidents are handled as per the severity.

•Review of online incident reports every quarterly is conducted by the senior leadership team and the core members of Online Safety group.

•Based on overall review of e-safety in the school that happens every year the management and school leadership shall decide on updating the policies and practices and bring into picture improvements.

Schools Sanctions

Separate sanctions (as mentioned in the Acceptable Use Policy) are in place for staff and students when there is breaches in what is deemed as acceptable.

Data Protection

As a school, IPHS is in possession of a lot of personal information of its staff and students.

The Data Protection Policy of the school is put in place to protect such data and assure stake holders of responsible handling of such data. Following guidelines are ensured while working with sensitive data:

•Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

•Employees are not allowed to take personal/sensitive data of any other person off campus (or to make unofficial copies). Sanctions will be applicable if such breach is revealed.

•Use such data only for the purpose for which access is provided.

•When printing or photo copying personal data, ensure that only authorized personnel will be able to access the same.

•Do not send personal information via email, instant message, chat or any unsecured file transfer unless it is encrypted.

•Backups of confidential data are always subject to the same restrictions as the original data

The commitment of the school when collecting and using personal data is as below:

•Inform individuals why the information is being collected

•Inform individuals and gain consent when their information is to be shared with any entity other than the Ministry of Education or any Govt.agency where sharing of such information is legally allowed/required.

•Ensure that information is not retained for longer than necessary

•Ensure that when obsolete information is destroyed that it is done so appropriately and securely.

•Breach of data protection policy shall be considered gravely and dealt with in accordance with the sanctions as mentioned in the policy (Reference Data Protection Policy)

Media Consent

Whenever a new student joins school at the time of admission parents shall sign a media consent form where the parent permit the school to use their wards images/works in school's social media sites, website as well as videos. Parents always have the option of refusing to sign the form where in the school shall refrain from using that student's images.

Internet Access for Visitors and Guests

Visitors shall be provided with a separate controlled access to the School Wi-Fi, with limited access as set by the school. Once connected to the IPHS network, all visitors shall be required to strictly follow the security requirements of IPHS. This password for the same shall be changed every month in case of Front Desk guests. In case of other guests such as trainers, inspectors etc., the password would be changed once their usage during that visit is completed.

Monitoring and Intervention of Online Safety Incident

IPHS strives to build a culture of being digitally safe. For this it encourages pupils, staff and parents to engage with technology in a productive, and positive manner. At the same time, it is important to have a balance between allowing freedom to explore and use digital tools to their full potential and installing strong controls. In order to ensure this IPHS has a well-structured monitoring and intervention strategies

Filters and Authorized Monitoring

•Through fire walls and filters the usage of the digital infrastructure is limited to what is considered acceptable by the school (Reference: Acceptable Use Policy).

•Internet access is filtered age appropriately and as per UAE norms.

•IT equipment shall be audited regularly (based on pre-fixed schedules) by the IT Coordinator

•Over and above regular digital devices audit, the school reserves the right to inspect any and all usage of technology devices, digital resources, and network infrastructure provided by the school as well as user owned devices if used on school network, with or without prior notice, in the case of a suspected malpractice/breach.

•Regular audit of password strength statistics shall be done and maintained by the IT coordinator. (Reference: school password policy). Audit of sensitive data handled by HR, Accounts would be done by the IT coordinator with prior notice and in the presence of the respective department head to ensure the effective data handling and security of the system. Reports on such audits will be shared with respective department heads and corrective action designed by the department head and online safety leader where required.

•Alerts shall be set in case users accessing the blocked sites and repeated offenders shall be reported to the safety leader for further action.

•Incident reports and logs shall be shared with the online safety leader.

COMMUNICATION TECHNOLOGIES

A wide range of rapidly developing communications technologies has the potential to enhance learning.

	Staff & other adult				***Students/Pupils***			
COMMUNICATION TECHNOLOGIES	Allowed	Allowed at certain times	Allowed for selected staff	Not Allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not Allowed
Mobile phones may be brought to the school	✓							✓
Use of mobile phones in lessons				✓				✓
Taking photos on mobile phones or other devices		✓	✓					✓

Use of instant messaging			✓					✓
Use of Social networking sites		✓						
Use of blogs				✓				✓

When using communication technologies the school considers the following as good practice:

- The official school communication portal (NASCORP) may be regarded as safe and secure and is monitored. Staff should therefore use only the school portal to communicate with parents.
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such communications.
- Any digital communication between staff and pupils or parents / carers (email, chat, portal etc) must be professional in tone and content.

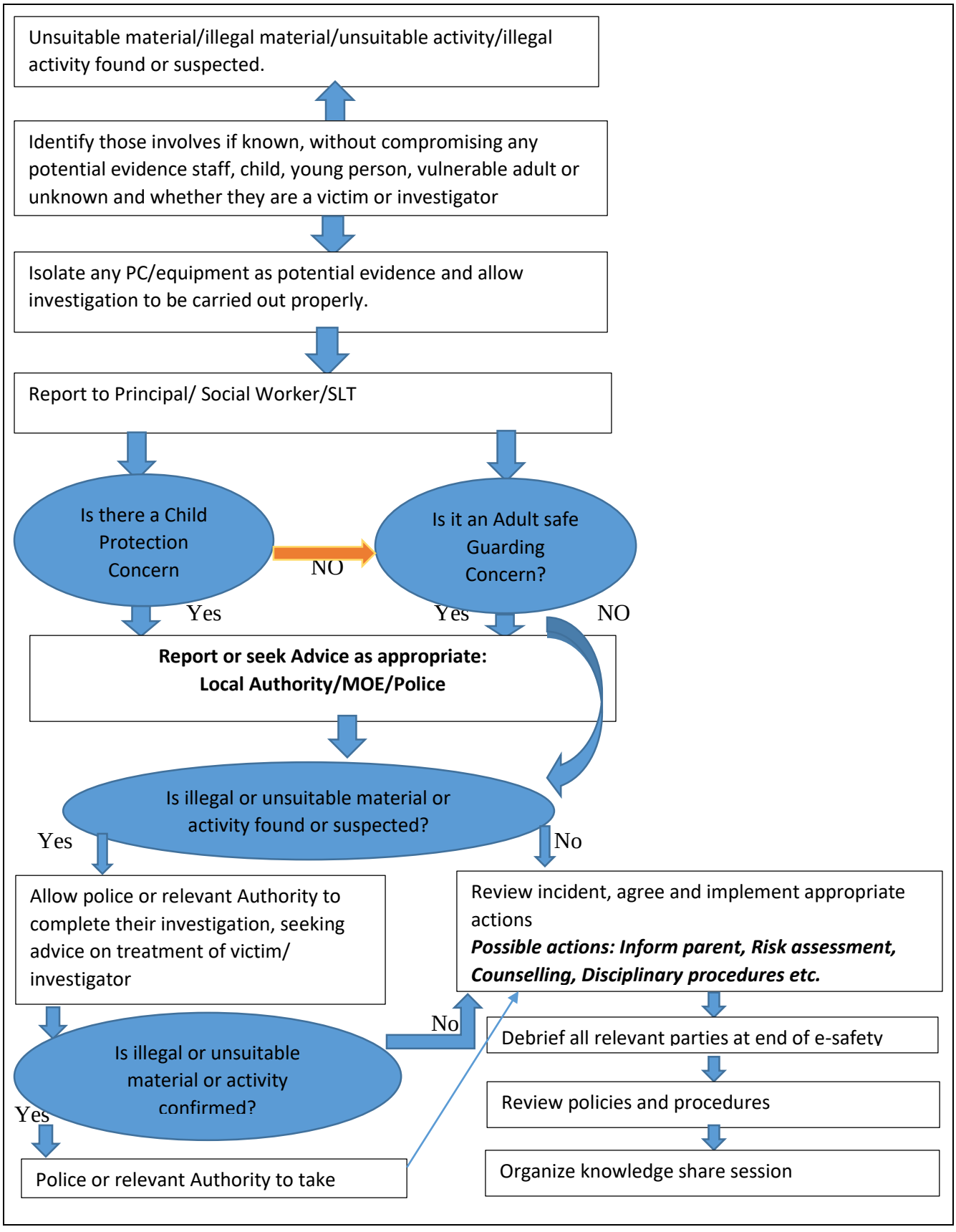
  Unsuitable / inappropriate activities

  The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:
Unacceptable & Illegal Activities
child sexual abuse images
promotion or conduct of illegal acts, eg. under the child protection, obscenity, computer misuse and fraud legislation
adult material that potentially breaches the Obscene Publications Act in the UAE
criminally racist material
Pornography
promotion of any kind of discrimination
promotion of racial or religious hatred
threatening behaviour, including promotion of physical violence or mental harm
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
Using school systems to run a private business
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions

Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
Creating or propagating computer viruses or other harmful files
On-line gaming (educational)
On-line gaming (non-educational)
On-line gambling

MANAGING E-SAFETY INCIDENTS – FLOW CHART



Emergency Contact Details for Reporting

School stakeholders can always approach the school directly or seek help from the following when there is an incident.

School Contact Details

Office: 07 2223214

Mail Ids: Online safety Leader- -

School Counselor/Social Worker – counsellor@iphsrak.com