IBN SEENA ENGLISH HIGH SCHOOL

ONLINE SAFETY POLICY

Reviewed By	**Senior Leadership & Management Team**
Date	**APRIL 2020**

1. AIM

The aim of the School is to ensure that all students are safe and the wellbeing of all students is a school priority. The school has developed an effective online safety strategy to protect all learners.

The Aim of the policy is to -

a) To protect the whole School community from illegal, inappropriate and harmful content or contact;
b) To educate the whole School community about their access to and use of technology; and
c) To establish effective mechanisms to identify, intervene and report to higher authorities when required.

This policy applies to all members of the School community, including staff and volunteers, students, parents and visitors, who have access to the School's Technology in school or at home

The school has these policies in addition to other policies, to the School's online safety practices:

a) Acceptable Use Policy for Students
b) Safeguarding and Child Protection Policy
c) Anti-Bullying Policy
d) Risk Assessment Policy for Student Welfare
e) Staff Code of Conduct
f) Computing Policy
g) Mobile Device usage policy
h) Acceptable Use of Photographs and Video Policy

These policies procedures and resource materials are available to students and staff on the school website.

This is a whole School policy.

2. ROLES AND RESPONSIBILITIES

2.1 The Governing Body

a) The Governing Body as proprietor has overall responsibility for safeguarding arrangements within the School, including the School's approach to online safety and the use of technology within the School.
b) The Governing Body is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of students.
c) The Governing Body will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies.

2.2 Principal and Senior Leadership and Management Team

a) The Principal and SLT has overall responsibility for the safety and welfare of members of the School community.
b) The E Safety officer with the e safety team and senior members of staff from the Senior Leadership will lead responsibility for safeguarding and child protection. The responsibility will include managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding & Child Protection Policy.
c) The team will work with the Head of ICT (To be appointed) and the IT Manager (to be appointed)in monitoring Technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of students.
d) The team will regularly monitor the Technology Incident Log maintained by the IT Manager.
e) The team will regularly update other members of the SLT on the operation of the School's safeguarding arrangements, including online safety practices.

2.3 IT Manager

a) The IT Manager, together with his team, is responsible for the effective operation of the School's filtering system so that students and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.
b) The IT Manager is responsible for ensuring that:
    1. The School’s Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;
    2. The user may only use the School’s Technology if they are properly authenticated and authorised;
    3. The School has an effective filtering policy in place and that it is applied and updated on a regular basis;

4. The use of the School's Technology is regularly monitored to ensure compliance and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and
5. Monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

c) The IT Manager will provide details on request outlining the current technical provision and safeguards in place to filter and monitor inappropriate content and to alert the School to safeguarding issues.

d) The IT Manager will report regularly to the SLMT on the operation of the School's Technology. If the IT Manager has concerns about the functionality, effectiveness, suitability or use of Technology within the School, s/he will escalate those concerns promptly to the appropriate members(s) of the School's Senior Leadership Team (SLT).

e) The E Safety Officer and IT Manager is responsible for maintaining the Technology Incident Log and bringing any matters of safeguarding concern to the attention of the Principal and SLT.

2.4 E- Safety Leader

a) Establish and maintain a safe ICT learning environment within the school.

b) Promote the importance of e-safety within school and to ensure the safety of their pupils and staff.

c) Ensure policies and procedures that incorporate online safety concerns are in place, Acceptable Use Agreements are reviewed annually.

d) Ensure the whole school community is aware of what is safe and appropriate online behaviour and understand the sanctions for misuse.

e) Work with the E-safety team and ensure that training is available for staff, students and parents to feel informed and know where to go for advice

f) Work with staff to ensure that appropriate online safety education is embedded throughout the curriculum.

g) Work alongside the ICT TEAM to ensure that filtering is set to the correct level for staff, children and young people.

h) Training children to stay safe online, both in school and outside of school.

i) Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified.

j) Evaluate the delivery and impact of the settings online safety policy and practice

2.5 E- Safety Committee

a) Representatives are responsible for the implementation of the E-Safety policy and for reviewing the effectiveness.

b) Providing training and advice for teachers, students, staff and parents.

c) To ensure that all new staff and pupils are aware of its content and have acknowledged appropriate 'Acceptable Use Policy' and attend regular meetings with the E-safety leader.

d) Ensuring that all staff is aware of the procedures that need to be followed in the event of an E-Safety incident taking place and maintaining an E-Safety incident log book.
e) Regular updates on the monitoring of E-Safety incidents and reporting to the leader.
f) They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices.

2.6 All staff

a) The School staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the School's policies and of safe practice with the students.
b) Staff are expected to adhere, so far as applicable, to the policies of the school.
c) Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding & Child Protection Policy to Child Protection Officer, Supervisors and Principal.

2.7 Parents

a) The role of parents in ensuring that students understand how to stay safe when using Technology is crucial. The School expects parents to promote safe practice when using Technology and to:
   - ➢ support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;
   - ➢ talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behavior; and
   - ➢ encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support

b) If parents have any concerns or require any information about online safety, they should contact the Supervisors / E Safety officer.

2.8 Students

a) Students should adhere to the policies of the school
b) Should avoid plagiarism and uphold copyright regulations
c) Should understand the risks associated with the use of internet
d) Should understand the importance of reporting abuse, misuse or access to inappropriate materials
e) Should report any concerns in line with the School's policies and procedures
f) Should be a good digital citizen

3 EDUCATION AND TRAINING

3.1 Students

a) The safe use of Technology is integral to the School's well-being. Students are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile devices.

b) Technology is included appropriately in the lessons and students are encouraged to use ICT in their HW or research tasks at home.

- ➢ Example --children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;
- ➢ Children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, debates, elocution, role-play etc.
- ➢ Children are guided to recognise that a range of technology is used in places such as homes and Schools and encouraged to select and use correct technology for particular purposes.

c) The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/pastoral activities, teaching students:

- ➢ about the risks associated with using the Technology and how to protect themselves and their peers from potential risks;
- ➢ to be critically aware of content they access online and guided to validate accuracy of information;
- ➢ how to recognise suspicious, bullying, and extremist behaviour;
- ➢ the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- ➢ the consequences of negative online behaviour; and
- ➢ How to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and how the School will deal with those who behave badly.

d) The School's Acceptable Use of ICT Policy for Students sets out the School rules about the use of Technology including internet, email, social media and mobile electronic devices, helping students to protect themselves and others when using Technology. Students are reminded of the importance of this policy on a regular basis.

3.2 Staff

a) The School provides training on the safe use of Technology to staff so that they are aware of how to protect students and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur.

3.3 Parents

a) Information is available to parents via portal, email and school website.
b) Orientation is conducted for parents as and when required.
c) Parents are encouraged to read the Acceptable Use Policy for Students with their son/daughter to ensure that it is fully understood.

3.4 Useful resources

a) There are useful resources about the safe use of Technology available via various websites including:

- http://www.thinkuknow.co.uk/
- http://www.saferinternet.org.uk/
- https://www.internetmatters.org/
- http://educateagainsthate.com/
- http://www.kidsmart.org.uk/

4. ACCESS TO THE SCHOOL'S TECHNOLOGY

a) The School provides internet and intranet access and an email system to students and staff as well as other Technology. Students and staff must comply with the respective Acceptable Use of Technology Policy when using School Technology. All such use is monitored by the IT Manager and his/her team.

b) Students and staff require individual user names and passwords to access the School's internet and intranet sites and email system which must not be disclosed to any other person. Any student or member of staff who has a problem with their user names or passwords must report it to the IT Department immediately.

c) No laptop, tablet or other mobile electronic device may be connected to the School network without the consent of the IT Manager. All devices connected to the School’s network should have current and up-to-date anti-virus software installed and have the latest OS updates applied. The use of any device connected to the School's network will be logged and monitored by the IT Support Department.

d) The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the IT Department.

e) The school does not have a policy of students bringing mobile to school unless in an emergency and informed to class teacher and supervisor. The school does not have a policy of BYOD for students. Students have access to desktops only in the computer lab.

5. USE OF PERSONAL DATA, PHOTOGRAPHS AND VIDEO

Students, staff, parents and students need to be aware of the risks associated with publishing digital images on the internet. The school is informed about the necessity to educate users about these risks and have implement policies to reduce the likelihood of the potential for harm: Staff are permitted to take digital/video images on school devices, for educational purposes e.g. for classroom displays, projects & as evidences of class activities

a) When taking digital/ video images teachers should ensure that the students are appropriately dressed and are not positioned/posed in a way that bring the individual or the school into disrespect
b) Digital images/ video images should not be manipulated or amended. However it is acceptable to crop an image.
c) Students must not take, use, share or publish images of others without consent
d) Parents are permitted to take photographs of their children, for their own private use. However the school should provide guidance for parents and to make it clear that any images taken must be for private use only according to the Data Protection legislation
e) School Authorities will seek the consent of parents regarding the use of student images on the School Website.
f) Parents may at any time withdraw their consent/ non consent for the use of student's images and videos in school published materials or on the school website.

6. PERSONAL DATA PROTECTION

All Personal data including photographs and videos will be recorded, processed, used and stored according to the Data Protection Act 1998.

a) All personal data will be fairly obtained and lawfully processed in accordance with the legislation.
b) Every effort will be made to ensure that data held is accurate and up to date.
c) All photographs and video content are classified as personal data under the Data Protection Act.
d) Images or video content may be used for any school purposes only after getting informed consent from the parents. Parents are responsible for providing consent on their child's behalf and they have the right to withdraw consent at any time.
e) Images obtained by the school will not be kept for longer than necessary.
f) Copies of photos and video recordings held by the school will be annotated with the date on which they were taken and will be stored securely.
g) They will not be used other than for their original & intended purpose.
h) No digital image will be altered or enhanced in any way without prior permission by the Supervisor.

7. ACCEPTABLE USE POLICIES

To ensure that all stake holders are fully aware of their responsibilities, the school's Acceptable Use policies (Staff, Students & Parents) are formulated for providing the stakeholders with an understanding of how they are expected to use technology in the organization and beyond. It is the responsibility of all stakeholders to read, understand and adhere to this policy.

If in case a stakeholder is found not complying with the terms of the AUP, depending on the sensitivity of the issue, the management will determine the degree of corrective actions to be taken.

Students, Parents and staff are made familiar with the ways of reporting these issues.

For students the disciplinary actions taken will be in liaison with the Behaviour Policy set by the Ministry of Education.

8. PROCEDURES FOR DEALING WITH INCIDENTS OF MISUSE

a) Staff, students and parents are required to **report incidents** of misuse or suspected misuse to the E Safety officer and Supervisors for immediate intervention.

b) **Misuse by students**
   - Anyone who has any concern about the misuse of Technology by students should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.

- Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection Officer and E Safety officer / Supervisor.

c) **Misuse by staff**

- Anyone who has any concern about the misuse of Technology by staff should report it to the Principal / Supervisor.

d) **Misuse by any user**

- Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the class teacher / supervisor / Principal.
- The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

9. MECHANISMS OF REPORTING ANY SUCH ABUSE OR MISUSE

a) The incident must be reported to the representative of the respective blocks, using the reporting format immediately, who in turn will report the cybersecurity incident to the E-Safety leader.

b) The E-Safety officer and the school IT department will assess the severity of the incident and resolve the issues or work to limit any future damage and preserve sensitive information.

c) Decisions may also need to be made about whether to request external assistance based on the nature of the security breach.

d) The IT team will need to identify what people were impacted by the incident or caused the incident; in some cases, a cyber incident may have been caused by a student who conducted malicious activity.

e) The school needs to identify how technology was impacted and address any issues. For example, does malicious software need to be uninstalled?

f) Finally, Policies may need to be revised or new ones implemented, to prevent future cyber incidents from occurring.

10. MONITORING AND REVIEW

a) All serious incidents involving the use of Technology will be logged centrally in the Technology Incident Log by the E Safety / IT Manager. / Supervisor

b) The Principal / SLT and E Safety team will have responsibility for the implementation and review of this policy and will consider the record of incidents involving the use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and online safety practices within the School are adequate.

c) Consideration of the effectiveness of the School's online safety procedures and the education of students about keeping safe online will be included in the Governors' annual review of safeguarding.

REVIEW

The policy has been reviewed and modifications have been made (E Safety Officer and E Safety Team) as per the E Safety requirements sent by SPEA.

February 2021