المدرسة الإسبانية في أبوظبي
The Spanish School of Abu Dhabi

E Safety Policy

Create and Review	Date	Approved
Andrea Hernández Pasek – HR Manager	August 2020	Dr. Laurent Bonardi – Founding Principal.
Andrea Hernández Pasek – HR Manager	August 2021	

- Protecting and educating students and staff in their use of technology.
- Informing teachers and parents/guardians about their role in safeguarding and protecting SSAD students at school and at home.
- Putting policies and procedures in place to help prevent incidents of cyber-bullying within the school community.
- Having effective and clear measures to deal with and monitor cases of cyber-bullying using our school platform Tootoot.

THE SPANISH SCHOOL OF ABU DHABI ENSURES THAT:

- Students will be made aware of acceptable and unacceptable Internet use.
- Students will be taught, where appropriate, to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Students will be educated about the effective use of the Internet.
- Students will be taught how to evaluate Internet content by teachers.
- Students will be taught how to report unpleasant Internet content to their class teacher.
- The school Internet access is designed expressly for student use and includes filtering appropriate to the needs of our students.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit.
- All students and staff understand the importance of password security and the need to log out of accounts.

SOCIAL NETWORKING AND PERSONAL PUBLISHING:

- The school has a duty of care to provide a safe learning environment for all its students and staff and will ensure the following:
- Blocking student access to social media sites within school boundaries
- Educating students about why they must not reveal their personal details or those of others, or arrange to meet anyone from an online site.
- Educating both students and staff as to why they should not engage in online discussion revealing personal matters relating to any members of the school community.
- Educating both students and staff about ensuring all technological equipment is always password/PIN protected
- Informing staff not to accept invitations from students or parents/guardians on social media
- Informing staff about regularly checking their security settings on personal social media profiles to minimize risk of access of personal information

PARENTS ROLE AT HOME.

- Keep the computer in a central place, where everyone can see what's on the screen.
- Stay involved (without stepping on their toes constantly) on what they are doing online – especially if it's got to do with searching and looking for new information etc.
- Tell them the "No-Can-Go" sites and "No-Can-Play" games rules ahead of time. Check out which sites they want to access, or which games they want to play and tell them if they are acceptable or no-go zones, until they reach a certain specified age.
- Set time limits. Giving kids unlimited access to online causes unlimited problems for parents. Tell them how many hours they have a week.
- Explain online habits. Explain strangers often play pretend games and they are not really who they claim to be.

- Switch Safe Search on as a setting. It's great that most inappropriate content does get filtered by Etisalat or du here in UAE, but there are many slip ups and search results may often have content that's not age appropriate.
- Remind them that they should not engage in any form of cyberbullying – even in jest. They should not do anything online that they would be ashamed of doing in real life.
- Beyond online, watch what content you have on your computer. Often we receive email that is not age appropriate for our children, but we leave that in our mailboxes or desktops. Set the example, clean up.
- If your children have started to do their homework online, or are gathering information, researching facts etc., explain to them clearly how they should not "copy and paste" (plagiarize) content for their homework, unless they mention sources etc. Their teachers should help them understand this, but you should make it clear that this is not on.
- Be involved. Be courteous. Be alert. Show on-going interest in what they are playing, reading, doing online. And always remind them that there is life (and a wonderful one) outside that screen.

PROCEDURES FOR REPORTING AND RESPONDING TO TECHNOLOGY MISUSE

Responding to Incidents of Misuse This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident.

In the event of suspicion, all steps in this procedure should be followed:

• Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

• Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

• It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

• Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below

• Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

➢ Internal response or discipline procedures
➢ Involvement by ADEK or national / local organization (as relevant).

➢ Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately.

Other instances to report to the police would include:

➢ Incidents of 'grooming' behaviour
➢ The sending of obscene materials to a child
➢ Adult material which potentially breaches the Obscene Publications Act
➢ Criminally racist material
➢ Other criminal conduct, activity or materials

• Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. It is important that all of the above steps are taken as they will provide an evidence trail for the school / academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school / academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with