SCHOOL SECURITY PLAN

Young people and technology are often inseparable in today's world. In order to provide a safe environment, we need to understand the types and frequency of risks and the solutions to eliminate them, or even better. To create a safer environment for young people, creating a safer Internet for younger users A significant amount of research has been done.

One of the risks that online young people face is cyberbullying or online victimization: that is, bullying or harassment using electronic forms of communication. Some examples of pepper bullying can be clearly defined, while others are less. in some cases it is only due to the bad behavior of a person. Pepper bullying usually requires the repetition of the action. There is a clear lack of agreement to spread the bully bullying, especially compared to traditional bullying, and this affects the statistics about its prevalence. and cyber bullying, the relationship between the tyranny and the cyber bullying. These attempts are considered to be potentially effective prevention measures to counteract offline bullying and can also be useful in countering bullying online.

Young people and adults often have different interpretations of online victimization. While adolescents tend to treat some actions in some way, young people can explain the same examples as a normal activity among their peers, but they start with an offline problem. These programs typically involve periodic assessments of their activities. Successful and effective programs work to promote anti-bullying strategies at all levels in the school, from individual pupils and classes, to anti-bullying teams that unite educators and students.

Heavy internet users can go online with inappropriate content, young people can often face sexual harassment or online exposure to sexual content. Unlimited content on the World Wide Web can lead immersed young people to a vast collection of unwanted sexual content and information. sexual conversations include sending or receiving sexual photos, or disclosing undesirable sexual information. In addition, when browsing the web for non-sexual content through unwanted pop-ups, young people sometimes face obscene content or sexual imagery / videos. receive mail fraud.

The most commonly proposed strategy for dealing with unwanted sexual encounters is to encourage or prevent them from blocking the online forum. For this reason, courses and informative interviews are usually organized by schools or local councils, while other efficient methods include filtering and firewall technologies. In addition, safer online environments for users of companies that provide internet access it is recommended that they encourage other means of dealing with online risks.

Many of the risks of the Internet can be reduced if young people are more proactively protecting their online privacy. They need to be trained and less informed about how to manage their personal information online, and they need to know how to manage their privacy, which is especially important in schools from a young age. There is a possibility of misunderstanding that may prevent them from trusting each other and thus cause an effective control of the online risk. Therefore, communication between young people and adults should be encouraged, and dialogue about cyber security can help to alleviate the gap and improve security measures. Such dialogues can also encourage young people to educate their parents about resources and websites online, Tomorrow, it is very important to discuss the Internet security measures among the leaders of the world. The benefits that the Web provides are part of our modern culture and we should not allow many of our technological advancements to backfire on the safety of young people themselves.

E ABOUT OUR SECURITY CURRENT

• Content related to the use of internet in media literacy and IT courses has been updated in the light of current and technological developments.

• Seminars are organized for the development of knowledge, skills and attitudes about the conscious and safe internet use in children.

 • Turkish, Health Information, Science, etc.

 • The updating of the subjects related to the conscious use of the internet, especially social media, with the updated information was provided by the school ICT coordinator teacher.

• There is a secure internet network by ICTA to ensure effective and safe use of technology during the execution and maintenance of the Fatih project.

• Emphasis is placed on electromagnetic pollution and internet security in schools affiliated to MoNE.

SAFETY PRECAUTIONS FOR CHILDREN AND ADOLESCENTS

 • We conduct awareness-raising activities for supervised, limited and purposeful use of children and adolescents.

• Ensuring the promotion and dissemination of packages related to the safe use of the Internet is state policy.

• Guidance is given to encourage the use of limited internet packages in homes.

• Priority is given to the lessons in order to develop practices related to usage awareness.

 • To raise awareness of parents about the ways of audit and technological facilities and to develop and disseminate the necessary practices. academics are assisted by the university.

MOBILE PHONE USAGE

For this reason, teachers and auxiliary services personnel cannot use their mobile phones in the time and environment of the students.

2. Students cannot bring their mobile phones when they come to school - they can come and go with the student service vehicle and it is easily possible to reach the student through the service staff. Students who are obliged to bring their mobile phones to the school for any reason must hand over their mobile phones to the school administration's location and the related officer in order to take them out of school. It is forbidden for any student to have a mobile phone in the class and therefore to use it.

3. The student who violates the prohibition of the possession of mobile phones in the classroom and in the school building is confiscated by the school administration (to be returned at the end of the period) for one week in the first violation and in the second violation for two weeks in the third violation. In order to support this sanction to be applied in case of violation of the rules, the parents shall be accepted and the parents shall be accepted at the beginning of the academic year (or during the registration of the student).

4. No student is allowed to access the wi-fi connection within the school boundaries. In other words, it is forbidden for the student to obtain the password and connect to the wireless network connection in any way. The student's cell phone, which is found to be in violation of this prohibition, is confiscated for a week.

5. The student's mobile phone can only be used under the control of the teacher and as a course tool during the course activity applications within the boundaries of the school and classroom. Use outside of this purpose is not permitted.

6. The student cell phone number is not allowed to be learned by anyone other than the student guardian.

7. Meetings are held with parents every year to inform them about the use of mobile phones at the beginning of the academic year.

8. Teachers are held three times a year (at the beginning, at the end and at the end of the training period).

Make sure your school has a clear photo and image policy, regardless of whether it is a legal requirement in your country

PHOTOGRAPHY OR VIDEO SHOOTING AND PUBLISHING IN OUR SCHOOL

1. Photographs and videos cannot be taken within the boundaries of the school or school playground, except for the events and programs that the parents of the parents want to know, except those assigned by the school administration. This prohibition also applies if a student wants to take pictures and videos of another student.

2. The photographs and videos taken by the persons appointed by the school administration may only be published in the school's official web address and virtual environments with the request and written approval of the relevant parent. Photos and videos of the pupil's student who does not approve his / her student will not be published.

3. Measures are taken to prevent psychological pressure during the shooting of students who are not allowed to photograph and video images by their parents.

4. The pictures and videos published by the school officials are not included in the personal information of the students. Students will ask for permission from a teacher before preparing or answering a video conference call or message. Video conferencing will be appropriately supervised for students' age and ability. (schools should list how this will be implemented and achieved.) The consent of parents and carers will be acquired before children participate in video conference activities. Video conferencing will take place through official and approved communication channels following a sound risk assessment. Only home administrators are given access to video conference management areas or remote control pages. Unique login and password information for trained video conferencing services will only be provided and secured to staff members.

E-SECURITY POLICY

Digital technologies also offer exceptional opportunities and opportunities for school-age children. Children can also access information, fun games and similar activities easily and quickly through the Internet. However, besides the great facilities provided by digital technologies, the existence of the danger of the child encountering traps with mental, spiritual and physical attacks is an unacceptable reality. For example, it is possible for a child on the Internet to watch a commercial that appears unintentionally, or to enter a pornographic site because of an incorrect word that he or she will knowingly write to the search engine; dragging to lower environments. Not to mention the fact that there is no news of a child who is frightened, anxious and terrified, mentally or physically victimized by some online games.

The most sure way to protect the child from the dangers mentioned above is to keep him away from the Internet. However, due to the rapidly developing digital technologies, and unfortunately, it is not possible to keep the child completely out of the internet, and to completely prohibit it does not solve the problem. Moreover, it has become impossible to completely prohibit and prevent access to the Internet because of environmental factors and parental attitudes. For this reason, it is necessary to find more effective measures than trying to completely ban the child from the dangers of the internet environment.

First of all, it should be noted that no measures that can be taken due to the possibilities of digital technologies will not protect the child from the above-mentioned hazards by one hundred percent. Therefore, there is no more effective way to protect the child from these dangers than to provide information, consciousness and behavior to the child.

Because of these facts, as a school policy, we conduct persistent and determined practices in order to protect our students from the dangers and damages of the Internet and provide necessary, applicable prohibitions:

E-SAFETY PRECAUTIONS FOR CHILDREN AND ADOLESCENTS

 • We carry out awareness-raising activities in order to provide controlled and limited use for children and adolescents.

• Ensuring the promotion and dissemination of the packages related to the safe use of the Internet is state policy.

• Guidance is given to encourage the use of limited internet packages in homes.

 • Family unions should be strengthened and encouraged.

 • There is a need to increase social projects in which young people will actively participate.

 • Help to expand the use of secure internet packages.

 • It is necessary for the computers used in the family to be able to create different profiles according to the user and the secure internet service should be offered with different packages according to these profiles. Studies on this have been started.

• Use-aware

SCHOOL STAFF

Staff will be aware that Internet traffic can be monitored and tracked up to a single user. Dignity and professional conduct are required when using school systems and devices. All members of staff will be provided on a regular (minimum annual) basis in a variety of ways, with professional and personal, up-to-date and appropriate staff training on safe and responsible Internet use. All employees will realize that their online online behavior can affect their role and reputation in the school. Legal, disciplinary or legal measures may be taken, considering that it has made the profession or institution dangerous or lost confidence in its professional skills. Members of staff who are responsible for managing filtering systems or monitoring ICT usage will be supervised by the Leadership Team and have open procedures to report problems or concerns. The school must check the useful online tools that employees must use according to their age and abilities. Parents' attention will be directed to the school's online safety (e-Security) policy and expectations on the school website and in the school prospectus and on the school website. A cooperative approach to online safety with parents at home and at school will be encouraged. It can involve providing parental training with demonstrations and recommendations for safe Internet use at home or highlighting online security at other well-attended events. organize social activities such as parental education, time together and sports days. As part of the School Agreement, parents will be asked to read the online safety information. Parents will be encouraged to read the School's Acceptable Use Policy and discuss their impact with their children. Information and guidance for parents on online security will be presented to parents in various ways. Parents will be encouraged to behave positively in the role model for their children online.

     In 2017 and 2018, the school celebrated its safe day with efficient and comprehensive support for parents. Throughout the week, seminars, introductory banners and webinars have been enabled to participate actively. : //guvenlinet.org.tr/tr/

Secure Web (guvenliweb.org.tr) - awareness portal for online security issues.

Safe Kids (guvenlicocuk.org.tr) - a game and entertainment portal for children under 13 years.

Ihbar Web (ihbarweb.org.tr) - the phone line for illegal content.

Internet ICT (internet.btk.gov.tr) - Awareness portal on Internet and IT law.

SID Page (the gig.org.t) - Safer Internet Day, the official sayfası.vel and students are introduced, around the educational parent and student informative vidoe in Turkey, presentations izlenmiştir.oku has prepared presentations using the sort of Web2 tools, boards were hazırlanmıştır. with families. http://guvenlinet.org.tr/en/ for information purposes.

to provide direct interaction with children and young people on new technologies.

• include them in safer Internet-related activities.

• see their experiences and measure internet perceptions.

• Increase digital literacy and awareness on safer internet.