ILGIN SCIENCE AND ART CENTER
e-SECURITY (e-SAFETY) PLAN

Young people, children and technology have become an inseparable duo in today's technology age. As the use of the Internet increases in daily life, it has become essential to take precautions for safe use. In order to provide a safe environment, we need to understand the types and frequency of risks and find solutions to reduce them or eliminate existing risks, and understand the purposes of using the internet for young people and children. Considerable research has been done on the risks that young people face online, on ways to create a safer internet environment for younger users.

One of the risks that youth and children face while online is cyberbullying or online victimization: that is, bullying or harassment using electronic forms of communication. Some examples of cyberbullying are clearly identifiable, while others are less so. There may be cases where the language and tactics used by the cyber word to intimidate its victim are a clear sign that it is a criminal offense, and in some cases it is simply due to the bad behavior of a person. Cyberbullying often requires repetition of the action. There is a clear lack of agreement on the prevalence of cyberbullying, especially compared to traditional bullying, and this is affecting the statistics. One way to address cyberbullying on the Internet is to use the link between school bullying and cyberbullying. School bullying is referred to as attempts by young people to improve relationships and attitudes towards each other. Such initiatives are considered potentially effective prevention measures to counter offline bullying and may also be useful in countering online bullying.

Teens and adults often have different interpretations of online victimization. Adults tend to treat some actions in some way, while teenagers may explain the same instances as a normal activity among their peers, but these start with an offline issue. Schools establish policies to facilitate the establishment of a school-wide bullying prevention program, and these programs typically include periodic evaluations of their effectiveness. Successful and effective programs work to promote anti-bullying strategies at all levels in the school, from individual students and classrooms to anti-bullying teams that unite educators and students.

Internet users may encounter inappropriate content online; Teens are often exposed to sexual harassment or sexual content online. The unlimited content on the World Wide Web can lead immature teens to a vast collection of unwanted sexual content and information. Examples include solicitations for sexual intercourse, sexual conversations, posting or

soliciting sexual photos, or disclosing unsolicited sexual information. Also, when surfing the web for non-sexual content via unsolicited pop-ups, teens are sometimes confronted with obscene content or sexual imagery/videos. They can get email scams.

The most commonly recommended strategy for dealing with unwanted sexual encounters is to encourage or assist teens to block such providers or to leave the online forum where they are having trouble. Because many teens tend not to involve adults when they encounter embarrassment online because of embarrassment, parents and educators need to be made aware of signs to watch out for to indicate that teens may be facing challenges. Therefore, courses and informative talks are often organized by schools or local councils, while other effective methods include filtering and firewall technologies. In addition, it is recommended that companies providing internet access provide safer online environments for their users, thus promoting another way of addressing online risks.

Many of the risks posed by the internet can be reduced if young people more proactively protect their privacy online. They need to be trained to be less willing to expose personal information online and know how to manage their privacy; This type of education is important in schools, especially from a young age. Due to the generation gap between parents and their children, there is a possibility of misunderstanding which can prevent them from trusting each other and thus lead to effective control of online risk. Therefore, communication between young people and adults should be encouraged; Engaging in a cybersecurity dialogue can help alleviate the gap and improve security measures. Such dialogues can also encourage young people to educate their parents about online resources and websites.

It's crucial to discuss internet security measures tomorrow among the world's leaders. The benefits of the web are part of our modern culture and we should not let our many technological advances backfire on the safety of young people themselves.

ABOUT OUR E SECURITY CURRICULUM

• The content related to internet use in media literacy and informatics courses has been updated in the light of current and technological developments. In our institution, e-twinning projects related to Media Literacy are carried out. (see : https://twinspace.etwinning.net/95775/home)

• Seminars are held to develop children's knowledge, skills and attitudes about conscious and safe internet use.

• Turkish, Health Sciences, Sciences etc. are taught appropriately in related courses.

• The school informatics teachers provided updating the course curricula with renewed information on the subjects related to the conscious use of the internet, especially the social media.

• A secure internet network is available by BTK to ensure effective and safe use of technology during the execution and maintenance of the Fatih project.

• Electromagnetic pollution and internet safety are given importance in schools affiliated to MEB.

SAFETY MEASURES FOR CHILDREN AND ADOLESCENTS

• We carry out awareness raising activities regarding family-oriented children and adolescents to provide them with controlled, limited and purposeful use.

• It is government policy to promote and spread packages related to safe use of the Internet.

• Guidance is given to encourage the use of limited internet packages at home.

• This subject is given priority in the lessons in order to develop applications for usage awareness.

•To raise awareness of parents about control methods and technological possibilities, and to develop and disseminate necessary practices. Assistance is sought from academics from the university.

USE OF MOBILE PHONE

Therefore;

1. Teachers and auxiliary services personnel cannot use their mobile phones when and where students are present.

2. Students cannot bring their mobile phones when they come to school, as it is easily possible to come and go by the student bus and it is easily possible to reach the student through the shuttle staff. Students, who have to bring their mobile phones to school for any reason, have to deliver their mobile phones to the place indicated by the School administration and to the relevant officer, in a closed form, to be picked up after school. It is forbidden for any student to have and therefore use a mobile phone in the classroom.

3. The student who violates the ban on keeping a mobile phone in the classroom and in the school building will be confiscated by the school administration (to be returned at the end of the period) for one week in the first violation, two weeks in the second violation, and throughout the term in the third violation. In order for the student's parent to support this sanction that will be applied in case of violation of the rules, a written agreement made at the beginning of the academic year (or during the student's registration) is accepted and signed by the parent.

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 by any means and connect to the wireless network connection. The mobile phone of the student who is found to have violated this prohibition will be confiscated for one week.

5. The mobile phone can be used by the student within the boundaries of the school and classroom only during the course activities, under the control of the teacher and as a course tool. Uses other than for this purpose are not permitted.

6. The student's mobile phone number is not allowed to be learned by anyone other than those who are permitted by the student's parents.

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

8. In the general assembly of teachers held three times a year (at the beginning, middle and end of education) with teachers, discussions are held for evaluation purposes about school safety and thus mobile phone policy.

PHOTO OR VIDEO TAKING AND PUBLISHING AT OUR SCHOOL

1. Photos and videos cannot be taken within the boundaries of the school and the school garden, except for the activities and programs that the parents of the students want to know, and by persons other than those assigned by the school administration. This prohibition also applies if a student wants to take a photo or video of another student.

2. Photos and videos taken by the people assigned by the school administration can only be published on the official website and virtual environments of the School with the request and written approval of the relevant student's parents. Photos and videos about the student of the parent who does not give consent for the student will not be published.

3. Precautions are taken to prevent students from experiencing psychological pressure during the shooting if their parents do not approve the photograph and video footage to be taken and published.

4. Personal information of students is not included in the pictures and videos published by school officials. Students will seek a teacher's permission before preparing or answering a video conference call or message. Video conferencing will be moderated appropriately for students' age and ability. (schools should list how this will be implemented and achieved) Consent of parents and caregivers will be obtained before children participate in videoconferencing activities. The videoconferencing will take

place through formal and approved communication channels, following a sound risk assessment. Only key administrators are granted access to video conferencing management areas or remote control pages. Unique login and password information for trained video conferencing services will be provided and secured only to staff members.

OUR E-SECURITY POLICY

Digital technologies also offer extraordinary opportunities and opportunities for school-age children. Children can easily and quickly access information, fun games and similar activities with the help of the internet environment. However, in addition to these wonderful opportunities provided by digital technologies, the existence of the danger that the child will encounter mental, spiritual and physical attacks and traps is a reality that cannot be underestimated. To give an example, it is possible for a child on the internet to enter a pornographic site by watching an advertisement that appears unintentionally, or because of a wrong word that he will knowingly or unknowingly type into the search engine. In addition, an image that provokes a child's curiosity may drag him into environments that will endanger him mentally, emotionally or physically. Almost every day we hear about a child who has been mentally or physically victimized by certain online games that frightens, worries and terrifies parents!

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

First of all, it should be stated that due to the possibilities of digital technologies, no measures that can be taken will not be able to protect the child one hundred percent from the above-mentioned dangers. Therefore, there is no more effective way than giving the child knowledge, awareness and behavior and making efforts for this goal in order to protect himself from the dangers in question.

Due to these facts, as a school policy, we persistently and decisively implement practices and impose necessary and applicable prohibitions in order to protect our students from the dangers and harms of internet environments:

E-SAFETY MEASURES FOR CHILDREN AND ADOLESCENTS

• We carry out awareness raising activities regarding family-oriented children and adolescents to provide them with controlled, limited and purposeful use.

• It is government policy to promote and spread packages related to safe use of the Internet. Telekom offers a secure internet package for this.

• Guidance is given to encourage the use of limited internet packages at home.

• It is necessary to strengthen and encourage school-parent unions.

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

• It should be helped to spread the use of secure internet packages.

• Computers used in the family should be suitable for creating different profiles according to the user, and secure internet service should be offered with different packages according to these profiles. Studies on this have been started.

• This subject is given priority in the lessons in order to develop applications for usage awareness.

SCHOOL STAFF

They attend the trainings organized by the European Schoolnet (www.eun.org) every year. Our school staff are trained by the ICT coordinator. All school staff and students, within the scope of Tübitak Science Talks, Assoc. Dr. He participated in the training on "I'm Safe Because I Know the Internet" by Utku Köse. Ayşegül Ümmühan Şan and Eda Karaca received Online Safeti MOOC training. They also participated in online and online professional development activities from the eTwinning professional development portal. The online safety (eSafety) policy will be formally provided and discussed for the participation of all employees and will be strengthened and highlighted as part of our responsibility to protect. Staff will be aware that Internet traffic can be monitored and traced to a single user. Discretion and professional behavior is required when using school systems and devices. All members of staff will be provided, professionally and personally, with up-to-date and appropriate staff training on safe and responsible Internet use in a variety of forms on a regular (at least annual) basis. Employees will all realize that their online behavior can affect their role and reputation in the school. Legal, disciplinary or legal measures may be taken if something is thought to have made the profession or organization dangerous or has lost confidence in their professional abilities. Members of staff responsible for managing filtration systems or monitoring ICT usage will be overseen by the Leadership Team and have clear procedures for reporting issues or concerns. School staff should check useful online tools to

use according to students' age and abilities. Recognizes that parents/caregivers have an important role to play so that children can become safe and responsible users of the internet and digital technology. Parents' attention will be directed to the school's online safety (eSafety) policy and expectations on newsletters, letters, school prospectus and school website. A collaborative approach to online safety with parents at home and school will be encouraged. It may include providing parent trainings with demonstrations and recommendations for safe Internet use at home, or emphasizing online safety at other well-attended activities. They will organize social events such as parent trainings, spending time together and sports days. As part of the School Agreement, parents will be required to read the online safety information. Parents will be encouraged to read the School's Acceptable Use Policy and discuss its implications with their children. Information and guidance for parents on online safety will be available to parents in a variety of formats. Parents will be encouraged to role model positive behaviors for their children online.

Safe internet day was celebrated in our school in 2022 and 2023 with effective and comprehensive parent support. Active participation was ensured in seminars, promotional posters and webinars throughout the week. Teachers of our school have shared on the e twinning portal, safer internet SID 2018 facebook and twitter accounts. Safer Internet Center (gim.org.tr) - Official page of Safer Internet Center.http://guvenlinet.org.tr/tr/

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

Safe Child (guvenlicocuk.org.tr) - Game and entertainment portal for children under 13 years old.

Warning Web (ihbarweb.org.tr) - hotline for illegal content.

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

SID Page (gig.org.tr) - Safer Internet Day official page in Turkey. Parents and students were introduced, informative videos and presentations of educational parents and students were watched. In our arrow, presentations were prepared using various web2 tools, and the boards were prepared together with the families. The http://guvenlinet.org.tr/tr/ page has been used for information purposes.

Direct interaction with children and young people on new technologies was ensured, participation in activities related to safer internet was ensured, and digital literacy and awareness on safer internet were increased.