2023-2025 EDUCATIONAL YEAR

LUTFİYE ALİ ŞADİ ÇELİK SECONDARY SCHOOL E-SAFETY PLAN

Children and technology are often inseparable in today's world. While the use of the web is increasing, it is also related to its safe use.To ensure a safe environment, we need to understand the types and frequency of risks and solutions to reduce them or even better, to eliminate them. A significant amount of research has been done on the ways to create a safer internet for younger users about the risks faced by children online.

One of the risks faced by online children is cyberbullying or online victimization: that is, bullying or harassment using electronic forms of communication. In some cases, it is caused by only one person's bad behavior. Cyberbullying often requires repetition of action.There is a lack of clear agreement on spreading cyberbullying a lack of clear agreement on spreading cyberbullying, especially compared to traditional bullying, and this affects statistics about its prevalence. One way to address cyberbullying on the internet is to use the link between school bullying and cyberbullying.Initiatives that try to improve attitudes and attitudes are considered as potentially effective prevention measures to counter offline bullying and can also be useful in countering online bullying.

Children and adults often have different interpretations of online victimization. While adults tend to somehow treat some actions, Children can explain the same examples as a normal activity among their peers, but they start with an offline problem. Schools create policies that will facilitate the creation of a school wide bullying prevention program, and these programs typically include periodic reviews of their activities. Successful and effective programs work to promote anti-bullying strategies at all levels, from individual students and classes,to anti-bullying teams that connect educators and students.

Many of the risks posed by the internet can be reduced if children more proactively protect their privacy online. They need to be trained to be less willing to reveal their personal information online and know how to manage their privacy; this type education is especially important in schools from a young age. Due to the gap, there is a possibility of misunderstanding that can prevent them from trusting each other and thus lead to effective control of online risk. Therefore, communication between children adults should be encouraged; engaging in cyber security dialogue can help ease the gap and improve security measures. Such dialogues can also encourage children to educate their parents about online resources and websites. It is very important to discuss internet security measures among the world's leaders tomorrow.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 children themselves.

ABOUT OUR E-SAFETY CURRICULUM

1. Content related to internet usage in informatics lessons has been updated in the light of current and technological developments.

2. Seminars are organized to develop the knowledge, skills and attitudes regarding the use of conscious and safe internet in children.

3. It is provided to be processed appropriately in the relevant courses in Turkish, Social Studies, Science etc.

4. Updating the subjects related to the conscious use of the internet, especially social media, to the curriculum with renewed information was provided by the school ICT coordinator teacher.

5. There is a secure internet network by BTK to ensure effective and safe use of technology during the Fatih project implementation and maintenance phase.

6. Electromagnetic pollution and internet security are given importance in schools which depends on National Ministry of Education .

E-SAFETY PRECAUTIONS FOR CHILDREN AND ADOLESCENTS

1. We carry out awareness-raising activities to ensure that children and adolescents for the family can provide controlled, limited and purposeful use.

2. It is government policy to ensure the promotion and dissemination of packages related to the safe use of the Internet.

3. Guidance is provided to encourage the use of limited internet

packages in homes.

4. This subject is given priority in lessons to develop applications for

usage awareness.

5. Raising awareness of parents about their control paths and technological possibilities, and developing and expanding necessary practices. Assistance is received from academics from the university.

USING MOBILE PHONE

1. For this reason; Teachers and assistant staff cannot use their mobile phones in the time and environment of the students.

2. Students who have to bring their mobile phones to school for any reason must deliver their mobile phones in a closed manner to the location indicated by the school administration and to the relevant official, at the exit of the school. It is forbidden for any student to have a cell phone in the classroom and therefore use it.

3. 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 in any way and connect to the wireless network connection.

4. Within the boundaries of the school and classrooms, the mobile phone can be used only during the course activity applications, under the control of the teacher and as a teaching tool. Uses other than this purpose are not allowed.

5. Student mobile phone numbers are not allowed to be learned by anyone other than those allowed by the student guardian.

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

7. In the general assembly of teachers, held three times a year with teachers (at the beginning, middle and end of education), discussions are held to evaluate school security and, therefore, mobile phone policy. Your school has a clear photo and image policy.

PHOTOGRAPHY OR VIDEO SHOOTING AND PUBLISHING IN OUR SCHOOL

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

2. Students' personal information is never included in the pictures and videos published by the school staff. Students will ask for a teacher's permission 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 to implement and achieve this) Consent of parents and carers will be obtained before children participate in video conference activities. Video conferencing will take place through formal and approved communication channels, following a sound risk assessment. Only main administrators are given access to video conferencing management areas or remote control pages. Unique login and password information for trained video conferencing services will be provided only to staff members and secured.

OUR E-SAFETY 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 internet environment. However, in addition to these wonderful possibilities provided by digital technologies, the existence of the danger that the child will face mental, spiritual and physical attacks and traps is also an undeniable reality. It is not day after that, we may not have heard about a child who has been physically or physically victimized by some online games, frightening, worrying and terrifying parents!

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

First of all, it should be stated that any precaution that could be taken due to the possibilities of digital technologies will not be able to protect the child one hundred percent from the dangers mentioned above. Therefore, there is no more effective way to protect the child from these dangers than to gain knowledge, awareness and behavior, and to strive for this goal.

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

E-SAFETY PRECAUTIONS FOR CHILDREN AND ADOLESCENTS

 1. We carry out awareness-raising activities to ensure that children and adolescents for the family can provide controlled, limited and purposeful use.

2.It is government policy to ensure the promotion and dissemination of packages related to the safe use of the Internet.

3. Guidance is provided to encourage the use of limited internet

packages in homes.

4. This subject is given priority in lessons to develop applications for

usage awareness.

5.Raising awareness of parents about their control paths and technological possibilities, and developing and expanding necessary practices. Assistance is received from academics from the university.

yönelik uygulamalar geliştirmek için derslerde bu konuya öncelik

verilmektedir.

SCHOOL STAFF

They attend the trainings held every year by the European Schoolnet (www.eun.org) and have certificates. Our school staff are trained by ICT coordinator. The online security (e-Security) policy will be officially provided and discussed for the participation of all employees and will be strengthened and highlighted as part of our responsibility for protection. Staff will be aware that internet traffic can be monitored and traced to a single user. Discretionary and professional behavior is required when using school systems and devices. Up-to-date and appropriate staff training on safe and responsible internet use will be provided to all members of the staff professionally and personally on a regular (at least annual) basis in a variety of ways. All employees will realize that their online behavior may affect their role and reputation at school. Law, discipline or legal measures can be taken if it is thought that something that has made the profession or institution dangerous, or that it has lost confidence in its professional abilities. Members of staff responsible for managing filtering systems or monitoring ICT usage will be supervised by the leadership team and will have clear procedures to report problems or concerns. The school should check useful online tools that employees should use based on students' ages and abilities. It recognizes that parents have an important role to play in order for children to be reliable and responsible users of the internet and digital technology. Parents' attention will be directed to the school's online safety (e Security) policy and expectations on the bulletins, letters, school prospectus and school website. The collaborative approach to online security with parents at home and at school will be encouraged. It may include providing parenting trainings with demonstrations and suggestions for safe Internet use at home, or highlighting online safety in other well attending events. They will organize social events such as parent trainings, spending time together and sports days. As part of the School Agreement, parents will be asked to read the safety information online. Parents will be encouraged to read the School Acceptable Use Policy and discuss its effects with their children. Information and guidance for parents on online security will be offered to parents in a variety of ways. Parents will be promoted role model positive behaviors for their children online.

Safe internet day was celebrated in our school in 2020 with the support of effective and comprehensive parents.

Secure 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.

Ihbar Web (ihbarweb.org.tr) - Hotline for illegal content.

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

SID Page (the gig.org.t) - Safer Internet Day official page in Turkey. Introduced to parents and students, educational parent and student informative videos and presentations were watched. Presentations were prepared using various web2 tools and panels were prepared with families. http://guvenlinet.org.tr/tr/ page is used for information purposes.