



ALEMDAĞ EMLAK KONUT SECONDARY SCHOOL e-Safety Policy and Integration to Curriculum

With the rapid development of technology, it was inevitable that every school had a School Security Policy. Because stakeholders can access the Internet in a variety of ways from the school building today. As a part of our daily lives, we all live with digital technologies. To ensure that our children know how to best use the opportunities available through digital technologies, it is now necessary to know and understand how to use them. In order to ensure that this is done in the safest and safest possible environment, we have a clear and concise Safe Internet School Policy that attracts our students' attention at home, at school or outdoors, or when they are alone.

E-SECURITY CURRICULUM INTEGRATION POLICY:

1. In our school, there is an interactive board and Fatih internet access network in all areas of lecture. In the lectures, eba education portal is frequently used. Fatih internet access network is used with network security filter.
2. Our school has a web site, it does not have social networks such as Facebook and Instagram.
3. Interactive boards are used in the control of teachers with security setup. Seminars are organized for students to develop their knowledge, skills and attitudes about the use of conscious and safe internet. Students are provided with proper processing in the related courses.
4. In our school, cell phones are kept in closed position during the lessons and they are placed in a special section for phones.
5. E-Security brochures are distributed to all school teachers, students and parents by the Information Technology Teacher. Seminars on topics such as ICT dependency, correct and safe use of ICT, and cyber bullying are regularly organized by the guidance service. These seminars are provided by ICT experts and / or police officers.
6. In our school, there are fixed panels for correct and safe use of ICT.
7. Due to the intensive use of interactive boards, conqueror access network and eba education portal in our school, accurate and safe use of ICT in each group by the teachers of teachers decisions are taken and the students are informed in this direction.
8. The teachers of our school received distance and face-to-face trainings on the issues of cyber bullying, correct and safe use of ICT by the Ministry of National Education.
- 9.. Safer Internet Day "is celebrated in our school.

10. On the website of our school, on e-security, <https://www.esafetylabel.eu/> site and videos and posters for students and parents quoted here. Our school stakeholders can get information about the subject at any time.

11. At our school's safe internet day celebrations, information brochures from the <https://www.esafetylabel.eu/> site are distributed in the seminars about the subject.

12. Internet ethics and secure internet use are taught to our students in the information technologies course.

13. In our school, 21st century communication skills are considered. In this regard, the students are encouraged to develop ICT usage skills.

14. In our school, awareness-raising activities are carried out on our stakeholders about becoming a digital citizen.

15. E-Twinning projects provide safe internet studies and students are aware of the use of secure internet.

16. Our work is on the e-Twinning portal.

17. The school administration and our teachers are guided to eTwinning on line training eba platform and encouraged to complete e-security training.

PURPOSE OF E-SECURITY POLICY IN OUR SCHOOL;

- Protect and secure all members of our SCHOOL online.
- To raise awareness of the potential risks and benefits of technology to the managers, teachers and staff of ALEMDAĞ EMLAK KONUT SECONDARY SCHOOL.
- Ensure that all staff work safely and responsibly, model positive behaviors online, and be aware of the need to manage their own standards and practices when using technology.
- Describe the procedures to be used explicitly when responding to online security concerns known to all members of the school.
- This policy applies to all staff, including the governing body, teachers, support staff, external contractors, visitors, volunteers, and other persons serving or on behalf of the school (collectively referred to as staff in this policy), as well as children and ensure that parents cover

As a result, our main goal is to ensure that this security policy is valid for use of information communication devices, including Internet access and personal devices. The same applies to students, staff or other persons, as well as devices provided by the school for remote use, such as laptops, tablets or mobile devices.

ALL EMPLOYEES RESPONSIBILITIES:

- o Contribute to the development of online security policies.
- o To be responsible for the security of school systems and data.
- o To be aware of a number of different online security issues and to know how they can be associated with children in their care.
- o Modeling best practices when new and emerging technologies are used.
- o Associate your online safety training with the curriculum as possible.
- o Identifying individuals concerned by following school protection policies and procedures and taking appropriate measures.
- o Emphasizing positive learning opportunities.

- o Take personal responsibility for professional development in this field.
- o eTwinning online trainings eba platform, especially e-Security training to continue.

MAJOR RESPONSIBILITIES OF STUDENTS ARE:

- o Contribute to the development of online security policies.
- o Read the School's Acceptable Use Policies and stay connected to them.
 - To respect the feelings and rights of others online and offline.
- o Ask for help from a trusted adult if things go wrong and support others facing online security issues.
- o Take responsibility for protecting themselves and others online.
- o To be responsible for their own awareness and learning about opportunities and risks of new and emerging technologies.
- o To be safe and responsible to assess and limit the personal risks of using certain technology.

THE MAIN RESPONSIBILITIES OF THE PARENTS

- o Reading School Acceptable Use Policies, encouraging their children to adhere to this policy and ensuring that they are committed as much as possible.
- o Discuss online safety issues with children, support the school's online security approaches, and consolidate safe online behaviors at home.
- o Modeling the safe and appropriate use of technology and social media.
- o Identify changes in behavior that indicate that the child is in danger of being damaged online.
- o Ask for help or support from schools or other appropriate institutions if they and their children face problems or problems online.
 - o Contribute to the establishment of the school's online security policies.
- o Safe and appropriate use of school systems such as learning platforms and other network resources.
- o To be responsible for their own awareness and learning about opportunities and risks of new and emerging technologies.

