Beykoz Barbaros Hayrettin Paşa Mesleki ve Teknik Anadolu Lisesi

eSafety Label

SCHOOL SAFETY PLAN

2022

PURPOSE

The purpose of the eSafety Label School Security Plan is to determine the terms of use and acceptable use policy of Information Systems in Beykoz Barbaros Hayrettin Paşa Vocational and Technical High School. In this context;

- To protect and secure all teachers, administrators, students and other employees of our school online and to raise awareness
- Ensuring that all staff work safely and responsibly, model positive behavior online, and be aware of the need to manage their own standards and practices when using technology.
- Define procedures to be used explicitly when responding to online safety concerns known to all members of the school.
- Ensuring that this policy applies to all personnel, including the governing body, teachers, students, parents, support staff, external contractors, visitors, volunteers, and others (collectively referred to as 'personnel' in this policy) who serve or perform on behalf of the school.
- Sonuç olarak ana hedefimiz, internet erişimi ve kişisel cihazlar da dahil olmak üzere As a result, our main goal is that this security policy applies to internet access and use of information communication devices, including personal devices. It also applies to school-issued devices for remote use by children, staff or others, such as laptops, tablets or mobile devices where they work.

OUR e-SAFETY POLICY:

- There is an interactive whiteboard and a secure internet access network in every area where lectures are given in our school. In lectures, eba education and eTwinning portals are also used. Secure internet access network is used with network security filter.
- Our school has a website, social networks such as facebook and instagram. The data published on these networks is shared in a controlled manner.
- Interactive whiteboards are used under the control of teachers with security installation.
- In our school, students' mobile phones are kept switched off from the time they enter the school, and they are placed in a special section made for telephones as long as the school continues.

- Seminars on ICT addiction, correct and safe use of ICT, and Cyberbullying are organized regularly for 9th, 10th, 11th and 12th grades by the guidance service.
- There are fixed boards in our school regarding the correct and safe use of ICT.
- Due to the intense use of interactive boards, secure access network and eba education and eTwinning portals in our school, decisions are made by the teachers of the group regarding the correct and safe use of ICT in each group, and the transfer of the quotations to the lessons and assignments (use of resources) and the students are informed in this direction.
- The teachers of our school have received/will receive remote and face-to-face training on Cyberbullying and the correct and safe use of ICT given by the Ministry of National Education.
- “Safer Internet Day” is celebrated in our school.
- Our school's website contains links on e-security, guvenliweb.org.tr, and videos and posters for students and parents quoted from here.
- Our school stakeholders can get information about the subject whenever they want.
- Guvenliweb.org.tr in safe internet day celebrations in our school and seminars on the subject. Information brochures taken from the website are distributed.
- In the Computer Science course, internet ethics and safe internet use are taught to our students.
- 21st century communication skills are considered important in our school. In this regard, efforts are being made to improve our student’s ICT usage skills.
- Efforts are made to raise awareness of our stakeholders about being a digital citizen in our school.
- It is strictly forbidden to take photos without permission in our school.
- The faces of the students of our school will not be displayed clearly on any social media site belonging to the school and in the project pictures within the eTwinning portal.
- The personal information provided by our students and parents when registering with our school is protected by and under the responsibility of the administration.
- Contact information of our parents can never be shared with third parties except for their own knowledge and wishes.

SCOPE:

This policy covers all users who have been granted access to all Beykoz Barbaros Hayrettin Paşa Vocational and Technical Anatolian High School Computer Systems and Information Technology services from inside or outside the school.

RESPONSIBILITIES:

The administration is responsible for the implementation of this policy.
Beykoz Barbaros Hayrettin Paşa Vocational and Technical Anatolian High School E-Security Board is responsible for the preparation and updating of this policy.

a) Key Responsibilities of All Employees Are:

- Contribute to the development of online security policies.
- Read and adhere to Acceptable Use Policies (AUPs).
- Being responsible for the security of school systems and data.
- Be aware of a range of different online safety issues and how they can relate to children in their care.

- Modeling good practices when using new and emerging Technologies
- As much as possible link curriculum with online safety education.
- Identifying individuals of concern and taking appropriate action by following school protection policies and procedures.
- Emphasizing positive learning opportunities.
- Taking personal responsibility for professional development in this field.

b) The Major Responsibilities of Children and Young People Are:

- Contribute to the development of online security policies.
- Read and adhere to the School's Acceptable Use Policies.
- Respecting the feelings and rights of others online and offline.
- If things go wrong, seek help from a trusted adult and support others who encounter online safety issues.
- At a level appropriate to their individual age, abilities and weaknesses:
- Take responsibility to protect themselves and others online.
- Being responsible for their own awareness and learning regarding the opportunities and risks posed by new and emerging technologies.
- Acting safely and responsibly to assess and limit the personal risks of using a particular technology.

c) Main Responsibilities of Parents Are:

- Read the School's Acceptable Use Policies, encourage their children to adhere to it, and ensure that they do, as appropriate.
- Discussing online safety issues with their children, supporting the school's approaches to online safety, and reinforcing appropriate safe online behaviors at home.
- Modeling the safe and appropriate use of technology and social media.
- Identifying changes in behavior that indicate that the child is at risk of harm online.
- Seeking help or support from the school or other appropriate agency if they or their children encounter problems or problems online.
- Contributing to the establishment of the school's online safety policies.
- Safely and appropriately use school systems such as learning platforms and other network resources.
- Being responsible for their own awareness and learning regarding the opportunities and risks posed by new and emerging technologies.

DEFINITIONS:

Computer Systems

Computer systems refers to all kinds of computer-related hardware, equipment and intellectual property. This includes computer systems, personal computers, mobile devices, computer networks and any software, firmware, operating software and application software owned, leased, adapted or controlled by the School. . For the sake of clarity, “computer systems” includes local network, cloud or Internet-based services adapted by the School, or general local network, cloud or Internet-based services used to store School activities or School data.

BASIC PRINCIPLES:

Terms of Use

By using the School's computer systems, all users agree that the School makes no representations about the confidentiality of any messages or data stored in or sent through such systems; They accept that the School reserves the rights set forth in this document and that the use of the said systems is limited to the School-approved purposes, and that the necessary notifications have been made to them. The use of the School's computer systems in connection with School activities and personal use in matters of no importance is not a right, but a privilege granted to limited members of the School's community. Therefore, the School may at any time and without notice block access to all or part of its computer systems (for all or some users) in whole or in part. The users of the computer systems of the School must comply with this Beykoz Barbaros Hayrettin Paşa Vocational and Technical Anatolian High School Acceptable Use Policy and that they have accepted and will comply with the Acceptable Use Policy by using the said systems, and that they have been notified in this regard, and They acknowledge that they have given their consent for the School to enforce the Acceptable Use Policy. Users also agree that they will comply with the relevant legislation and refrain from any behavior that will put the School under liability. The School reserves the right to change this Beykoz Barbaros Hayrettin Paşa Vocational and Technical Anatolian High School Acceptable Use Policy and other conditions regarding the use of computer systems at any time without prior notice and to take actions that are required or appropriate to be taken in accordance with the relevant legislation. To protect the integrity of the School, the School's computer systems and its users against unauthorized or improper use of the facilities in question, and to identify possible uses that may result in violation or violation of the School's rules and policies; reserves the right to limit or prevent any person's use without notice, and to search, copy, remove or modify any data, file or system resource that may harm the appropriate use of a computer system or be used in violation of the School's rules or policies. . Beykoz Barbaros Hayrettin Paşa Vocational and Technical Anatolian High School reserves its rights regarding periodic control of systems and all other rights for the protection of computer systems. Malware scanning systems in e-mail messages processed on computers, smart boards, servers, and school servers are examples of controls for protection purposes.

The school is not responsible for the work it will carry out to ensure the confidentiality and security of the said systems, data loss that may occur due to system malfunction or any other reason, or interference with files.

a) Managing School/Website

- The contact information on the website will be the school address, e-mail and phone number. Personal information of staff or students will not be published.
- The Head of School will take overall editorial responsibility for the online content posted and ensure that the information is accurate and appropriate.
- The website will comply with the school's publication guidelines, including accessibility, respect for intellectual property rights, privacy policies, and copyright.
- E-mail addresses will be carefully published online to avoid spam mails.
- Student work will be published with the permission of the students or their parents.
- The administrator account of the school website will be protected with a suitably strong password.
- The school will post information about protection on the school website for members of the community, including online safety.

b) Posting Images And Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the school image use policy.
- The School will ensure that all images and videos are included in accordance with other policies and procedures such as data security, Acceptable Use Policies, Code of Conduct, social media, use of personal devices and mobile phones.
- In accordance with the image policy, written consent of the parents will always be obtained prior to the electronic publication of students' pictures/videos.

c) Use of Personal Devices and Cell Phones

- Widespread ownership of mobile phones and other personal devices among children, youth and adults requires all members to take steps to ensure responsible use of mobile phones and personal devices .
- The use of mobile phones and other personal devices by children, teenagers and adults will be decided by the school and included in appropriate policies, including the school Acceptable Use or Cell Phone Policy.
- Our school is aware that personal communication with mobile technologies is an accepted part of daily life for children, staff and parents; however, it requires the safe and appropriate use of such technologies in school.

d) Students' Use of Personal Devices and Cell Phones

- Students will receive training in the safe and appropriate use of personal devices and mobile phones.
- It is strictly forbidden to use information tools without the knowledge and permission of the school administration and the teacher, by speaking, taking audio and video, sending messages and e-mails, and sharing them with their friends in a way that will adversely affect education and also to have a telephone during school lesson hours.
- Students are obliged to put their phones in the phone boxes made by the school administration before the lesson starts.
- In case of violation of the use of the mobile phone beyond its intended purpose, the student turns off the phone and gives it to the teacher in order to protect the private data on the phone. The course teacher delivers the student's phone to the relevant assistant principal. The mobile phone is kept in a safe place until it is handed over to the student's parents. The phone is not handed over to anyone other than the parent.
- All use of mobile phones and personal devices by children will be in accordance with the acceptable use policy. Cell phones or personal devices may not be used by students during classes or official school hours unless they are part of an approved and directed curriculum-based activity with a teacher's approval.
- The use of children's mobile phones or personal devices in the educational activity will take place when approved by the school administration.
- If a student needs to call their parents, they will be allowed to use the school phone.
- It is recommended that parents do not communicate with their children on their mobile phones during school hours and apply to the school administration. Exceptions may be permitted in exceptional circumstances as approved by the teacher.

- Students should only give their phone numbers to trusted friends and family members.
- Students will be taught the safe and appropriate use of mobile phones and personal devices, and the limitations and consequences will be recognized.
- If it is suspected that material on a student's personal device or mobile phone may be illegal or may provide evidence of a criminal offense, the device is handed over to the police for further investigation.

e) Use of Visitor Personal Devices and Mobile Phones:

- • Parents and visitors should use mobile phones and personal devices in accordance with the school's acceptable use policy.
- • Use of mobile phones or personal devices by visitors and parents to take photos or videos must be done in accordance with the school image use policy.
- • The School will provide and present appropriate signage and information to inform visitors about usage expectations.
- • Staff are expected to oppose problems when appropriate and safe and will always report any violations by visitors to management.

METHOD:

Acceptable Use Policy
Hundreds of users share our school systems. These systems should be used with caution; Even the misuse of a few people has the potential to disrupt the work of the School and others. For this reason, users should be careful and behave ethically when using the School's computer systems. This obligation includes but is not limited to the following::

- The School has all rights, ownership and interests in the computer systems of the School. Our school's acceptable use policy or any provision under the terms and conditions published by the School regarding the use of computer systems in no way means that such rights, property and interests are transferred to users. The School grants users a personal, worldwide, free, non-transferable, and non-exclusive license to use computer systems only. Users may not copy, modify, reproduce, create derivative works from, reverse engineer, disassemble, or otherwise decompile any software or other part of computer systems.
- Users cannot use computer systems that the School does not allow. Unauthorized use of computer systems by providing false or deceptive information or otherwise in order to gain access to computer systems is prohibited. Users may not use the School's computer systems to gain unauthorized access to the computer systems of other institutions, organizations or individuals.
- Users may not authorize anyone for any reason to use their School account. The account holder is responsible for any use of the school account. Users should take all reasonable precautions, including password protection and document protection, to prevent unauthorized use of their accounts. They should not share their passwords with another person and should change their passwords regularly. The account holder is responsible for any transaction performed using the password of a user account, even if the party performing the transaction is not the account holder himself.
- The School's computer systems should only be used for School-related matters as permitted. As with all School equipment, the use of computer systems, including the school network, for personal or commercial purposes is prohibited, unless expressly

permitted. The School's computer systems may not be used for any unlawful purpose, including, but not limited to, the collection, download, distribution of fraudulently or illegally obtained media documents and software. Use of external networks or services – including cloud services – must comply with acceptable use policies issued by both the University and the organizations providing such networks and services.

- Users may not access any information, School's software or other documents (including programs, subroutine library members, data and e-mail) without prior permission from the School's relevant personnel, information security officer or the relevant party; cannot modify, copy, move or remove such information, software and documents. Users may not copy, distribute, display or disclose third party software without prior permission from the licensor. Users may not install software that is not properly licensed for use on systems.
- No computer system belonging to the School may be used irresponsibly or in a way that interferes with the work of others. This; transmitting or making available content that is defamatory, offensive or harassing, as well as chain letters, unauthorized mass mailings, or unsolicited advertisements; deliberate, reckless or negligent damage to a system, material or information that does not belong to the user; deliberately interrupting electronic communications or otherwise violating the privacy of others or accessing information that does not belong to or is not for the user; including deliberate misuse or misuse of system resources; or downloading software or data into administrative systems from untrusted sources, such as freeware.
- The school is in no way responsible for the content that it does not provide to the computer systems itself. Users access content provided by others, accepting that they may consider it offensive, inappropriate or objectionable, and at the user's own risk. Computer systems are provided "As Is" and "As Available". The School disclaims any liability for the accuracy, completeness and reliability of third-party content. The user is responsible for the information he/she holds or stores on his/her computer systems.
- The user (i) attempts any action to prevent the operation of computer systems or the use of said computer systems by others; (ii) uploading content that will overload computer systems; (iii) actions that will endanger the general security of computer systems and/or harm other users; (iv) accepts that the use or attempt to use software that interferes with or interferes with the operation of computer systems is strictly prohibited.
- In case of detection of any information regarding the violation of this policy by another person, or an error or "bypass" of the security of computer systems, the incident must be reported to the E-Security Board.
- Unauthorized or improper use of School computer systems, including non-compliance with this policy, constitutes a violation of School policy and requires Disciplinary Board follow-up with the approval of the Administration. Any questions regarding this policy or its application to a particular situation are forwarded to the E-Safety Board.

REVIEW:

The responsibility for reviewing and updating this document rests with the Information Technologies Directorate. Changes and updates are published with the approval of the Administration. The review is done annually in June.

RESOURCES:

The following web addresses were used to determine the e-Security policy of our school, to provide trainings and to prepare the study plan..

- Official page of Safer Internet Center (https://ec.europa.eu/info/index_en)
- • Safer Internet Center (gim.org.tr)
- • Safe Web (guvenliweb.org.tr) - awareness portal for online security issues.
- • Safe Child (guvenlicocuk.org.tr) - Game and entertainment portal.
- • Warning Web (ihbarweb.org.tr) - hotline for illegal content.
- • eSafety Label School Safety Plan 2022 6 Internet BTK (internet.btk.gov.tr)