T.R.

YILDIRIM DISTRICT GOVERNORSHIP

YILDIRIM DISTRICT NATIONAL EDUCATION DIRECTORATE

ŞEHİT ZEKİ BURAK OKAY SECONDARY SCHOOL

E-SAFETY POLICY

ACCEPTABLE USE POLICY INFORMATION TEXT

- Our school is aware of the fact that e-security is an indispensable element for the protection of children and adults in the digital world where technologies such as computers, tablets and mobile phones are actively used. In this direction, necessary studies are carried out in our school.
- Believing that virtual platforms and information communication technologies are an important part of daily life, our school conducts supportive activities for children to learn the ways to manage the risks they face in the virtual environment, react to them and develop strategies.
- Our school has an obligation to provide quality internet access to the school community in order to raise educational standards, promote success, support the professional work of staff and improve management functions.
- Our school is responsible for ensuring that all our children and staff are protected from potential dangers in virtual environments.
- Our school has an interactive whiteboard and secure internet access network in every lecture area. EBA education and eTwinning portals are also used in lectures. Secure internet access network is used with network security filter.
- Our school has a website and social networks such as Twitter. Data published on these networks are shared in a controlled manner.
- Interactive boards are used under the control of teachers with security installation.
- In our school, students are not allowed to use phones without permission.
- By the guidance service, 5-6-7 and 8th grades are regularly informed about ICT addiction, correct and safe use of ICT, cyber bullying and seminars are organized.
- There are fixed boards in our school regarding the correct and safe use of ICT.
- Teachers of our school have / will receive online and face-to-face trainings on Cyber Bullying, the correct and safe use of ICT given by the Ministry of National Education.
- "Safer Internet Day" is celebrated at our school.
- Our school's website includes 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.
- In our school, information brochures quoted from guvenliweb.org.tr are distributed during safe internet day celebrations and seminars on the subject.
- Internet ethics and safe internet usage issues are taught to our students in the Information Technologies course.
- 21st century communication skills are important in our school. Related to this, studies are carried out to improve our students' ICT usage skills.
- In our school, activities are carried out to raise awareness of our stakeholders about being a digital citizen.
- It is strictly forbidden to take photos without permission at our school.
- The faces of our school's students will not be displayed clearly on any social media sites belonging to the school and in the project pictures within the eTwinning portal.
- The personal information provided by our students and parents while enrolling in 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 information and requests.

1. OBJECTIVE

The purpose of this e-Security policy; Şehit Zeki Burak Okay Secondary School determines the usage conditions and acceptable usage policy of computer systems and communication technologies. In this direction, our aims:

• Define the main principles expected from all members of the community to ensure that our school is a reliable environment where information technologies and internet ethics are used safely and responsibly.

• Protecting and ensuring the safety of all members of our school community online.

• Raise awareness among all members of our school community about the potential risks and benefits of technology.

• To ensure that all personnel work safely and responsibly, to model positive behaviors online, and to be aware of the need to manage their own standards and practices while using technology.

• Define procedures that are explicitly used in responding to online safety concerns known to all members of the school.

• This policy applies to all staff, including the governing body, teachers, students, parents, support staff, external contractors, visitors, volunteers and others who serve or fulfill the school's behalf (collectively referred to as 'staff' in this policy).

As a result, our main goal is to have this security policy applicable to the use of information communication devices, including internet access and personal devices. It also applies to school-given devices for remote use, such as laptops, tablets or mobile devices on which students, staff or other persons work.

2. CONTENT

This policy covers all users who are granted access to Şehit Zeki Burak Okay Secondary School computer systems and internet technologies from inside or outside the school.

3. RESPONSIBILITIES

The administration is responsible for the implementation of this policy.

The administration of Şehit Zeki Burak Okay Secondary School and the e-Security Commission are responsible for the preparation and updating of this policy.

A. The key responsibilities of all employees are:

- ✓ Contributing to the development of online security policies.
- ✓ Reading and adhering 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 know how they may relate to children in their care.
- ✓ Modeling good practice when using new and emerging technologies.
- ✓ Link curriculum to online safety education whenever possible.
- ✓ Following school protection policies and procedures to identify individuals who are concerned and take appropriate action.

- ✓ Maintaining a professional attitude level both indoors and outdoors in personal technology uses.
- ✓ Emphasis on positive learning opportunities.
- ✓ Taking personal responsibility for professional development in this area.

B. The main responsibilities of children and young people are:

- ✓ Contributing to the development of online security policies.
- ✓ Reading and adhering to Acceptable Use Policies (AUPs).
- ✓ 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 security issues.

At a level appropriate for their individual age, abilities and weaknesses:

- ✓ Taking responsibility for protecting themselves and others online.
- ✓ To be responsible for their own awareness and learning of the opportunities and risks brought by new and emerging technologies.
- ✓ To assess the personal risks of using a particular technology and to act safely and responsibly to limit those risks.

C. The main responsibilities of parents are:

- ✓ Reading to Acceptable Use Policies(AUP’s), encouraging their children to adhere to this policy, and ensuring that they adhere to it 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.
- ✓ Seek help or support from the school or other appropriate institutions if they or their children encounter problems or issues online.
- ✓ Contributing to the establishment of the school's online security policies.
- ✓ Using school systems such as learning platforms and other network resources in a safe and convenient way.
- ✓ To be responsible for their own awareness and learning of the opportunities and risks brought by new and emerging technologies.

4. DEFINITIONS

Computer Systems

Computer systems refer to all kinds of computer related hardware, equipment and intellectual property. This includes computer systems, personal computers, mobile devices, computer networks and all kinds of software, firmware, operating software and application software owned, rented, adapted, or owned, maintained or controlled by our school. For the sake of clarity, "computer systems" include local network, cloud or internet-based services adapted by our school, or general local network used to store school activities or school data, and cloud or internet-based services in their execution.

5. BASIC PRINCIPLES

Terms of Use

- ✓ All users, by using the School's computer systems accept that:

• The school does not make any statements about the confidentiality of any messages or data stored in or sent through these systems,

• The school reserves the rights specified in this document,

• The use of these systems is limited to school-approved purposes,

• The necessary notifications have been made in this regard.

- ✓ The use of the school's computer systems in relation to school activities and personal use in matters that are not important is not a right, but a privilege granted to limited members of the school community. Therefore, the school may block access to all or part of the computer systems (for all users or some users) completely or partially at any time and without any notice.
- ✓ The users of the computer systems of the school must comply with this Şehit Zeki Burak Okay Secondary School Acceptable Use Policy and by using the systems in question, they accept and comply with the Acceptable Use Policy; That they have been notified about the Acceptable Use Policy; They acknowledge that they allow the school to apply the Acceptable Use Policy.
- ✓ The users also accept that they will comply with the relevant legislation and refrain from any behavior that would put the School under obligation.
- ✓ The School reserves the right to change this Şehit Zeki Burak Okay Secondary School Acceptable Use Policy and other conditions regarding the use of computer systems at any time without prior notice, and to take the necessary or appropriate actions to be taken in accordance with the relevant legislation.
- ✓ Restricting or blocking the use of any person without notice, in order to protect all of the school's computer systems and users from unauthorized or improper use of the facilities in question, and to identify possible uses that would result in violation or violation of the school's rules and policies; and reserves the right to research, copy, remove or change any data, file or system resource that could impair the deemed appropriate use for computer systems or that could be used for violation of the school's rules or policies.
- ✓ Şehit Zeki Burak Okay Secondary School reserves the rights regarding periodic control of systems and all other rights for the protection of computer systems. Malware scanning in e-mail messages processed on school computers, smart boards, servers, and school servers are examples of controls for protection purposes.
- ✓ The school is not responsible for the efforts to ensure the confidentiality and security of the systems in question, data loss or tampering with files due to system malfunction or any other reason.

6. SAFER USE OF ONLINE COMMUNICATION AND TECHNOLOGY

A. Managing the School / Website

• Contact information on the website will be school address, e-mail and telephone number. Personal information of staff or students will not be published.

• The School Principal will take overall publication responsibility for published online content and ensure that the information is correct 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 posted 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 by appropriately encrypted with a 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 pictures and videos posted online are used in accordance with the school image use policy.

• The school will ensure that all images and videos are covered in accordance with data security, Acceptable Use Policies, Code of Conduct, social media, and other policies and procedures such as the use of personal devices and mobile phones.

• In accordance with the image policy, written consent of the parents will always be obtained before the pictures / videos of the students are published electronically.

C. Users

• Students will seek permission from a teacher before preparing or responding to a video conference call or message.

• Videoconferencing will be supervised appropriately for the age and ability of the students.

• Parents' consent will be obtained before children participate in videoconferencing activities.

• Video conferencing will take place through formal and approved communication channels, following a robust risk assessment.

• Only main administrators will be granted access to video conference management areas or remote control pages.

• Private login and password information for educational video conferencing services will be provided only to staff and will be kept confidential.

D. Content

• When recording a video conference lecture, written consent will be obtained from all sites and participants. At the start of the conference the reason for the recording must be stated and video conference recording must be available to all parties. Recorded materials will be stored securely.

• If third party materials are to be included, the school will check whether this recording is acceptable to avoid infringing on the third party's intellectual property rights.

• The school will establish a dialogue with other conference participants before joining a video conference. If they are not schools, the school will check that it has received the material appropriate for the classroom.

• Proper and safe classroom use of the internet and related devices.

• Internet use is an important feature of educational access, and all children will receive age- and ability-appropriate education as part of the integrated school curriculum to support and assist them in developing strategies to address their problems.

- Internet access of the school will be designed to develop and expand education.
- Internet access levels will be reviewed to reflect curriculum requirements and students' age and abilities.
- All members of staff are aware that they will not rely on filtering alone to protect children, and training in surveillance, classroom management and safe and responsible use is essential.
- Content will suit the age and abilities of the students.
- All school devices will be used in accordance with the school's Acceptable Use Policy and with appropriate safety precautions.
- Staff members will always evaluate websites, tools and apps before using them in the classroom or when recommending use at home.
- Students will be trained in the effective use of information for research on the Internet, including skills in locating, retrieving and evaluating information.
- The school will ensure that staff and students accept internet-derived material and copyright laws.
- Students will be taught to think critically before acknowledging the accuracy of information they have read or displayed.
- Evaluation of online materials is part of teaching and learning in all subjects and is seen as a whole in the curriculum.
- The school uses the internet to enable our students and staff to communicate and collaborate in a secure and confidential environment.

E. **Use of Personal Devices and Cell Phones**

- The widespread adoption of cell phones and other personal devices among children, teens and adults requires all members to take steps to ensure responsible use of cell 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 will be covered by the appropriate policies, including the School's e-Safety or Cell Phone Policy.
- Our school is aware that personal communication using mobile technologies is an accepted part of daily life for children, staff and parents; however, it requires such technologies to be used safely and appropriately in school.

F. **Prospects for the Safe Use of Personal Devices and Mobile Phones**

- Use of personal devices and mobile phones will be enforced in accordance with the law and other appropriate school policies.
- The responsibility of any electronic device brought to the field belongs to the user. The school takes no responsibility for any loss, theft, or damage to such items.
- The school accepts no responsibility for the potential or actual adverse health effects caused by such devices.
- Abuse or sending of inappropriate messages or content via mobile phones or personal devices is prohibited by any member of the community and any violation will be handled as part of the policy of discipline / behavior.

• All members of our school are recommended to take steps to protect their cell phones or devices from loss, theft or damage.

• All members of our school are advised to use passwords / pin numbers to ensure that unauthorized calls or movements cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers must be kept secret. Cell phones and personal devices should not be shared.

• All members of our school are advised to make sure that their mobile phones and personal devices do not contain any content that is offensive, disparaging or otherwise contrary to school / settings policies.

G. **Students' Use of Personal Devices and Cell Phones**

• Students will be trained in the safe and appropriate use of personal devices and mobile phones.

• It is strictly forbidden to use informatics tools in a way that adversely affects education and training by making speeches, taking sound and images, sending messages and e-mails, sharing them with friends without the knowledge and permission of the school administration and the teacher, and also to have a phone during school hours.

• All use of children's mobile phones and personal devices will be in accordance with the Acceptable Use Policy.

• Cell phones or personal devices cannot be used by students in lectures or official school hours unless students are in an approved and directed curriculum-based activity with the consent of a teacher.

• Children's use of mobile phones or personal devices in the educational event will only be possible when approved by the school administration.

• When 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 by mobile phones during school hours and contact the school administration. In exceptional cases, exceptions may be allowed 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 limits and consequences will be recognized.

• If it is suspected that material on the student's personal device or mobile phone may be illegal or provide evidence of a criminal offense, the device is handed over to the police for further investigation.

H. **Use of Personal Devices and Cell Phones by Personnel**

• Staff are not allowed to connect their personal phones or devices with children, young people and their families in a professional capacity, inside or outside the setting. Pre-existing relationships that will jeopardize this issue will be discussed with managers.

• Staff do not use personal devices such as cell phones, tablets or cameras to take photos or videos of children and only use equipment provided on the job for this purpose.

- Staff do not use any personal devices directly with children and only use equipment provided by the school during lessons / education activities.
- Staff will ensure that any use of personal phones and devices is always carried out in accordance with data protection and relevant school policy and procedures.
- Personal mobile phones and devices of the staff are turned off / silent during class hours.
- Bluetooth or other forms of communication should be "hidden" or turned off during class hours.
- In emergencies, personal cell phones or devices cannot be used during the academic year, unless permitted by the school administration.
- Staff will ensure that the content purchased on the site via mobile phones and personal devices is in line with their professional role and expectations.
- Disciplinary action is taken in cases where a staff member violates school policy.
- The police will be contacted if a staff member has illegal content stored or stored on a mobile phone or personal device or has committed a criminal offense.
- Any claim involving personal use by staff of mobile phones or devices will be responded to by following school management policy.

İ. Use of Visitors' Personal Devices and Cell Phones

- Parents and visitors must use mobile phones and personal devices in accordance with the school's e-Safety policy.
- The use of mobile phones or personal devices by visitors and parents to take photos or videos must be done in accordance with the school's picture use policy.
- The school will provide and present appropriate signage and information to inform visitors of their usage expectations.
- Staff are expected to confront problems when appropriate and safe, and will always report any violations of visitors to the administration.

J. Participation and Education of Children and Young People

- An online security (eSafety) curriculum is created to raise awareness among students about the importance of safe and responsible internet use and takes place throughout the school.
- Training on safe and responsible use will be given before internet access.
- Student contributions will be sought in writing and developing school online safety policies and practices, including curriculum development and implementation.
- Students will be encouraged to read and understand the Acceptable Use Policy, appropriate for their age and abilities.
- All users will be informed that network and internet usage will be monitored.
- Online safety (e-Safety) will be included in all courses, especially the Information Technology course, and will cover both safe school and home use.
- Online security (eSecurity) will be included in PSHE, SRE, Citizenshipand Computing / ICT programs and will cover both safe school and home use.
- E-Safety prospects and posters will be posted in all rooms with internet access.
- Safe and responsible use of the internet and technology will be strengthened in the curriculum and in all subjects.

• Outside support will be used to complement and support schools' internal approaches to online safety (eSafety) education.

• The school will reward students for their positive use of technology.

• The school will implement peer education to improve online safety in accordance with students' needs.

K. Participation and Training of Staff

• Online safety (eSafety) policy will be formally provided and discussed for the participation of all employees and strengthened and emphasized as part of our responsibility to protect.

• Staff will be aware that Internet traffic can be monitored and tracked to a single user. Discretion and professional behavior are required when using school systems and devices.

• All members of staff, professionally and personally, will be provided with up-to-date and appropriate staff training on safe and responsible Internet use in a variety of ways on a regular (at least annual) basis.

• All members of staff will realize that their online behavior can affect their role and reputation at school. Public, disciplinary or legal measures may be taken if something is thought to be found that puts the profession or institution in a state of corruption or has lost confidence in their professional abilities.

• Members of staff with responsibility for managing filtering systems or monitoring the use of ICT will be overseen by the Leadership Team and have clear procedures for reporting issues or concerns.

• The school highlights useful online tools that staff should use according to the age and abilities of the students.

L. Parental Participation and Education

• Our school recognizes that parents have an important role to play in helping children become reliable and responsible users of the internet and digital technology.

• Parents' attention will be directed to the school online safety (eSafety) policy and expectations on the school descriptions and school website.

• As part of our schools, parents will be asked to read online safety information.

• 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 safety will be made available to parents in a variety of formats.

• Parents will be encouraged to role model positive behaviors for their children online.

M. Responding to Online Incidents and Protection Issues

• All members of the school will be informed of the variety of online risks that can be encountered including sexting, online / cyberbullying, etc. This will be highlighted in staff training and educational approaches to students.

• All members of the school will be informed about the procedure for reporting online security (eSecurity) concerns such as filtering, sexting, cyberbullying, illegal content violation, etc.

• The Digital Subscriber Line (DSL) will be notified of any online safety (e-Safety) incident involving child protection concerns, which will be recorded later.

- Complaints about misuse of the Internet will be handled within the school's complaints procedures.
- Online / cyberbullying complaints will be handled within the scope of the school's anti-bullying policy and procedure.
- Any complaints about misuse of staff will be directed to the principal.
- The school complaint procedure will be communicated to students, parents and staff.
- Complaint and notification procedure will be notified to the staff.
- All members of the school should be aware of the importance of confidentiality and the need to follow formal school procedures to raise concerns.
- All members of the school will be reminded of safe and appropriate behavior online, and remind you of the importance of not posting any content, comments, pictures or videos that would cause harm, distress, or crime to any other member of the school community.
- The school manages online safety (e-Safety) incidents in accordance with the school discipline / behavior policy, when appropriate.
- The school notifies parents of any concerns as needed.
- Once any investigation is complete, the school will receive information, identify lessons learned, and implement changes as necessary.
- Parents and children need to work together with the school to solve problems.

7. METHOD

e-Safety Policy

Hundreds of users share the computer systems of Şehit Zeki Burak Okay Secondary School. These systems should be used with caution; Even the misuse of a few people has the potential to hinder the work of the school and others. For this reason, users should be careful and exhibit ethical behavior while using the school's computer systems. This obligation includes, but is not limited to:

- The School owns all the rights, property and interests in the computer systems of the School. No provision under Şehit Zeki Burak Okay Secondary School e-Safety Policy or the terms and conditions published by the school in any medium regarding the use of computer systems does not mean that ownership 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 convert any software or any other part of their computer systems to source code.
- Users cannot use computer systems that the school does not allow. Unauthorized use of computer systems by providing false or deceptive information or other means to gain access to computer systems is prohibited. Users cannot use the school's computer systems to gain unauthorized access to the computer systems of other institutions, organizations or individuals.
- Users cannot authorize anyone for any reason to use their school accounts. The account owner is responsible for any use of the school account. Users must take all reasonable measures, 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.

• School computer systems should only be used for School-related issues as permitted. As is the case for all school equipment, the use of computer systems, including the school network, for personal or commercial purposes is prohibited, except where expressly permitted. The school's computer systems cannot be used for any illegal purposes, including but not limited to collecting, downloading, distributing, fraudulently or illegally obtained media documents and software. Use of external networks or services - including cloud services - must comply with e-safety policies published by both the school and the organizations that provide such networks and services.

• Users cannot access any information, software or other documents of the school (including programs, subroutine library members, data and e-mail) unless they obtain prior consent from the school's relevant staff, information security officer or the relevant party; it cannot change, copy, move or remove such information, software and documents. Users may not copy, distribute, view or disclose software belonging to third parties, without the prior consent of the licensor. Users cannot install software on systems that has not been properly licensed for use.

• No computer system of the school can be used irresponsibly or in a way that interferes with the work of others. That includes content that is offensive, offensive or abusive; forwarding or making chain letters, unauthorized bulk mail or unsolicited advertisements available; deliberate, careless or negligent damage to a system, material or information not owned by the user; deliberate interruption of electronic communications or otherwise violating the privacy of others or accessing information that is not owned or intended for the user; the deliberate misuse of system resources or the misuse of others, or downloading software or data from unreliable sources such as free software to administrative systems

• The school is in no way responsible for content that it does not provide to computer systems in person. Users access content provided by others, accepting that they may consider them to be offensive, indecent or objectionable and at the user's own risk. Computer systems are provided "AS IS" and "AS AVAILABLE". The School releases itself from 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 computer systems.

• The user accepts that it is absolutely prohibited (i) any attempt to act to prevent the operation of computer systems or the use of such computer systems by others; (ii) uploading content that will overload computer systems; (iii) acts that pose a threat to the general security of computer systems and / or harm other users; (iv) use or attempt to use software that prevents or interferes with the functioning of computer systems.

• In the event that any information regarding the violation of this policy by another person or an error regarding the security of computer systems or a "by-pass" security is detected, the incident must be reported to the Şehit Zeki Burak Okay Secondary School administration or the School E-Security Commission.

• Unauthorized or improper use of school computer systems constitutes a violation of School policy, including failure to comply with this policy, and requires the Disciplinary

Board follow-up with the approval of the Administration. Any questions regarding this policy or its application to a certain situation are submitted to the school administration or to the E-Safety Commission.

8. REVIEW

The responsibility for reviewing and updating this document rests with the school administration. The changes and updates made are published with the approval of the Administration. The review takes place every year in June.

SCHOOL E-SAFETY COMMISSION

Gülçin RODOPLU	**Zehra BAŞARA**	**İdris DOĞRU**
English Teacher	**Counselor Teacher**	**Asistant Manager**

Serkan GÜCLÜ
School Principal