ACCEPTABLE USE POLICY INFORMATION TEXT

AIM

The purpose of this policy is to determine the terms of use and acceptable use policy of Vali Tahir Paşa Secondary School Computer Systems.

1. To protect and secure all members of our School online.
2. To raise awareness for the administrators, teachers, students and employees of Vali Tahir Paşa Secondary School about the potential risks and benefits of technology.
3. 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.
4. Define procedures to be used explicitly when responding to online safety concerns known to all members of the school.
5. This policy applies to all staff, including the governing body, teachers, students, parents, support staff, external contractors, visitors, volunteers, and others who serve or perform on behalf of the school (collectively referred to as 'staff' in this policy). to make it happen.
6. 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 (E-SAFETY) POLICY:

1. There is an interactive whiteboard and a secure internet access network in every area where lectures are made in our school. In lectures, eba education and eTwinning portals are also used. The secure internet access network is used with a network security filter.

2. Our school has a website. The data published on these networks is shared in a controlled manner.
3. Interactive whiteboards are used under the control of teachers with security installation.
4. In our school, students' mobile phones are kept closed from the moment they enter the school, and they are placed in a special section for phones as long as the school continues.
5. Seminars on ICT addiction, correct and safe use of ICT, and Cyber Bullying are organized regularly by the guidance service for grades 5-6-7 and 8.
6. There are fixed boards about the correct and safe use of ICT in our school.
7. Due to the intense use of interactive whiteboards, 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, transferring the quotations to the lessons and assignments (use of resources) and the students are informed in this direction.
8. The teachers of our school have received/will receive remote and face-to-face trainings on Cyberbullying and the correct and safe use of ICT, given by the Ministry of National Education.
9. "Safer Internet Day" is celebrated in our school.
10. About e-security on our school's website, guvenliweb.org.tr. There are links to the website and videos and posters for students and parents quoted from here.
11. In the Computer Science course, internet ethics and safe internet use are taught to our students.
12. 21st century communication skills are considered important in our school. In this regard, efforts are being made to improve our students' ICT usage skills.
13. In our school, awareness raising activities are carried out for our stakeholders about being a digital citizen.
14. Taking photos without permission is strictly prohibited in our school.

SCOPE

This policy covers all users who are given access to all Vali Tahir Paşa Secondary SchoolComputer Systems and Information Technology services from inside or outside the school.

RESPONSIBILITIES

The administration is responsible for the implementation of this policy. Vali Tahir Paşa Secondary School Information Technologies Directorate and E-Security coordinator are responsible for the preparation and updating of this policy.

KEY RESPONSIBILITIES OF ALL EMPLOYEES ARE:

- Contribute to the development of online security policies.
- Read and adhere to Acceptable Use Policies (AUPs).
- 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 the curriculum with online safety education.
- Identifying individuals of concern and taking appropriate action by following school protection policies and procedures.

KEY RESPONSIBILITIES OF CHILDREN AND YOUTH 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.

KEY RESPONSIBILITIES OF PARENTS ARE:

- Read the School's Acceptable Use Policies, encourage their children to adhere to this policy, and ensure that they do, as appropriate.
- Discussing online safety issues with their children, supporting the school's online safety approaches, and reinforcing appropriate safe online behaviors at home.
- Modeling the safe and appropriate use of technology and social media.
- Identifying changes in their 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.
- Contribute to the creation of the school's online safety policies.

MANAGING THE SCHOOL/WEBSITE

1. The contact information on the website will be the school address, email and phone number. Personal information of staff or students will not be published.
2. The Head of School will take overall editorial responsibility for the online content posted and ensure that the information is accurate and appropriate.
3. The website will comply with the school's publication guidelines, including accessibility, respect for intellectual property rights, privacy policies, and copyright.
4. E-mail addresses will be carefully published online to avoid spam mails.
5. Student work will be published with the permission of the students or their parents.

6. The administrator account of the school website will be protected with a suitably strong password.
7. The school will post information about protection on the school website for members of the community, including online safety.

USE OF PERSONAL DEVICES AND MOBILE PHONES

1. Widespread ownership of mobile phones and other personal devices among children, teenagers and adults requires all members to take steps to ensure responsible use of mobile phones and personal devices.
2. The use of mobile phones and other personal devices by children, teenagers and adults will be decided by the school and will be covered in appropriate policies, including the school Acceptable Use or Cell Phone Policy.
3. Vali Tahir Paşa Secondary 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.

ACCEPTABLE USE POLICY

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 cannot access any information, School 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.

E-SAFETY COMMISSION

Seren DEMİRTAŞ (English Teacher, e-Twinning & Erasmus + Coordinator)

Kader YURTAL (Maths Teacher, ICT Coordinator)

Sefer ÖZKAN (Headmaster)