# 

## E-SAFETY SCHOOL POLICY AND RULES

**AIM:**

* Şehit Teğmen Ertuğrul Platin Primary School, while using the internet, smart board, computer, laptop and mobile phones with its e-security studies; It aims to protect students, parents and teachers. • Since the internet and technology are an important part of

life, everyone should be made aware of learning methods for managing risks and developing strategies. • Our policy has been prepared for administrators, teachers, parents, all staff and students.

Applies to internet access and use of information communication devices.

## RESPONSIBILITIES:

* Contributing to the development of e-security policies. • Taking

responsibility for professional development during the positive learning phase. •

Taking responsibility for e-security to protect the school and those in it. • Using technology safely and responsibly. • Observing the danger in

case of damage and reporting it to the relevant units.

## SCHOOL WEBSITE:

* Şehit Teğmen Ertuğrul Platin Platin Primary School, our school's address, telephone, fax and e-mail address information is available on our website. • All

content published on our site is placed on the site by the IT unit after the approval of our school principal. • Our school's website is under the

responsibility of our IT unit and strong security measures have been taken. • Student works are published with the permission of

their parents.

# 

## SHARING IMAGES AND VIDEOS:

* All photos and videos shared are with the permission and approval of the school administration in accordance with school policy.

is shared. • Parental

permission is obtained for all posts containing student content. • Photographs

cannot be taken or used without the permission of the student as well as parental permission.

## USERS:

* Before a video to be prepared by students is prepared, tasks related to it Students must obtain permission from their teachers.
* For all shared student-based activities, parents' permission must be obtained before the activity. • Video conferencing will be done through official and approved sites. • Users cannot

share images of school students and employees on their personal social media accounts without approval by the school authorities.

**CONTENTS:**

* When video conferencing is held, it will be held through sites where all users can participate. • Before video conferencing, communication must be established with other schools. • All content that concerns/ includes school students and employees, but can only be controlled and approved

After going through the processes, it will be open to sharing.

## SAFE USE OF THE INTERNET AND COMPUTING DEVICES:

* Internet; While it has become one of the most important tools in accessing information, by associating it with the curriculum at school, we can provide our students and teachers with accurate information in the

safest way.

* We have integrated our internet access according to the age and abilities of our students. • We have secured all our school's IT devices by performing the necessary filtering in accordance with our usage policy. • All our

employees, parents and students have been

informed about the use of effective and efficient online materials. • E-safety and cyberbullying issues have been included in the annual plans of

certain courses, and this

Information transfer to students on these subjects continues throughout the year.

* Online materials are an important part of teaching and learning and are active within the curriculum. It is used as.
* 6 February Safe Internet Day is celebrated in our school. • Our school

fully implements security procedures in accordance with the law 5651, SOPHOS applications HARDWARE FIREWALL and a corporate ANTIVIRUS application are used. Additionally, HOTSPOT security measure for wi- fi is also included in the system. It is a system that requires an additional username and password after entering the password, and also requires the user's MAC address to be registered in the system.

# 

**USE OF MOBILE PHONES AND PERSONAL DEVICES:**

* Students are prohibited from using personal mobile phones during school hours. day pocket

Students who hand over their phones to the assistant principal receive their phones back at evening dismissal time.

* Students who do not hand over their mobile phones to the administration and take videos or photos with their mobile phones inside the school are subject to action in accordance with the law and the Reward and Discipline articles of the Secondary Education Institutions Regulation.
* The responsibility of all personal devices belongs to the individual. • Our school accepts the

negative health and legal responsibilities that may arise from the use of such devices.

It doesn't.

* Protection of our school's personal mobile phones and IT devices from loss, theft and damage takes all necessary precautions, but the responsibility belongs to the individual.
* Students of our school can use their school phones at a school when they need to call their parents.

They can use it under the supervision of the administrator.

* Our students are allowed to use their personal devices for educational purposes (use of web 2 tools, etc.).

must obtain permission from the school administration.

* Our parents are informed that they should not meet with their students during school hours. If there are compulsory situations, they should be allowed to meet with the school administration with permission.
* Our students are made aware that they should only share their mobile phone numbers with trusted people, and that they should not share personal information such as mobile phones with people they do not know or do not consider reliable.
* Employees (teachers, administrators, staff, etc.) must continue their duties by muting or turning off their personal mobile phones during class hours.
* If employees (teachers, administrators, staff, etc.) behave contrary to school policy, disciplinary procedures are initiated. • Institutional employees (teachers, administrators,

staff, etc.) and students bear legal responsibility for any content and messaging that they receive or send from students or institution employees via social media or chat programs. Any content or messaging that may be inappropriate is immediately reported to the school administration. It is shared with. Necessary precautions are taken to avoid such a situation.

# 

## E-SAFETY TRAINING:

* E-security curriculum for students is added to the annual plans of relevant courses and students informed about the issues.
* Internet usage of all users is monitored by the IT unit. This information has been communicated to all users.
* Guidance to improve online security in line with the needs of our students teachers implement peer education. • Students

who use technology positively will be rewarded. • The online security

policy will be officially announced to all our employees. • 6 February Safe Internet Day is celebrated in our school. School corridors for this day and

We have bulletin boards and social media posts in classrooms.

## ONLINE EVENTS AND PROTECTION:

* All members of our school will be informed about online risks. Training has been done

The contents will be announced.

* In our school, informative activities are carried out on issues such as illegal content, security violations, cyber bullying, sexual messaging, child abuse, and personal information security. • 6 February

is celebrated as Safe Internet Day. • All complaints

regarding misuse of internet, information technologies and equipment in our school

The school principal will be notified.

* All members of our school are official school members to eliminate privacy and security concerns.

They are informed to behave in accordance with the rules. • The school

is responsible for taking the necessary actions in case of negativities. • Employees

(teachers, administrators, staff, etc.), parents and students cooperate with the school to solve the problems.

must act together.

Veyis ŞAKRUCU

SCHOOL PRINCIPAL