E-SECURITY SCHOOL POLICY and RULES

Uşak High School Directorate

GOAL:

• Uşak High School Directorate, while using 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 the methods of managing risks and developing strategies.

• Our policy is prepared for administrators, teachers, parents, all staff and students, and applies to the use of internet access and information communication devices.

RESPONSIBILITIES:

• Contributing to the development of e-security policies.

• Taking responsibility for professional development in the positive learning phase.

• Taking responsibility for e-security to protect the school and its insiders.

• Using technology safely and responsibly.

• In case of damage, observing the danger and communicating it to the relevant units.

SCHOOL WEBSITE:

• As Uşak High School Directorate, our website has address, telephone, fax and e-mail address information.

• All content published on our site is put on the site by the IT department after being approved by our school principal.

• The website of our school is under the responsibility of our IT department and strong security measures have been taken.

• Student works are published with the permission of their parents.

SHARING IMAGES AND VIDEOS:

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

• Parents' permissions are taken for all student-related posts.

• In addition to the permission of the parents, the photograph of the student is not taken and used without the permission.

USERS:

• Before a video to be prepared by students is prepared, the students involved in this video should get permission from their teachers.

• Parents' permissions must be obtained prior to the event in all student-based shared activities.

• 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 the approval of the school authorities.
 CONTENT:
• During video conferencing, it will be held over sites where all users can participate.
• Communication with other schools must be established before video conferencing takes place.
• All content that concerns / involves school students and staff will only be open to sharing after they pass through the control and approval processes.

SAFE USE OF THE INTERNET AND IT DEVICES:
• Internet; While we have become one of the most important tools in accessing information, we are able to communicate this to our students and teachers in the safest way by associating it with the curriculum at the school.
• We have integrated our internet access according to the age and abilities of our students.
• We have secured all our information devices belonging to our school by making the necessary filters in accordance with our policy of use.
• All our employees, parents and students were informed about the use of effective and efficient online materials.
• E-security and cyberbullying issues are included in the annual plans of certain courses, and the transfer

of information to students on these issues continues throughout the year.

• Online materials are an important part of teaching and learning and are actively used in the curriculum.

• Safe internet day is celebrated in our school with various activities.

SECURITY TRAINING:

• The e-security curriculum for students is added to the annual plans of the relevant courses and students are informed about these issues.

• Counseling teachers apply peer education to improve online safety in line with the needs of our students.

• Students who use technology positively will be rewarded.

• Online security policy will be officially announced to all our employees.

• 6 February safe internet day is celebrated in our school. Today, billboard works and social media posts are made in the school corridors and classrooms.

USE OF MOBILE PHONES AND PERSONAL DEVICES:

• It is forbidden for students to use personal cell phones during school hours. Students who hand over their mobile phones to the deputy principal during the day take back their phones at check-out time.

• Students who do not deliver their mobile phones to the administration and take videos or photographs in the school with their mobile phones are subject to the Award and Discipline clauses of the Secondary Education Institutions Regulation.

• All kinds of personal devices are responsible for the person himself.

• Our school does not accept any negative health and legal responsibilities arising from the use of such devices.

• Our school takes all necessary measures to protect personal mobile phones and information devices from loss, theft and damage; but the responsibility belongs to the person.

• Our school students can use the phones belonging to the school under the supervision of a school administrator when they need to call their parents.

• Our students must obtain permission from the school administration to use their personal devices for educational purposes (use of web 2 tools, etc.). • 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 interview with the permission of the school administration. • Our students are made aware that they should only share their mobile phone numbers with trusted people and not share personal information such

as mobile phones with people they do not know.
• Employees (teachers, administrators, staff, etc.) should continue their duties by muting or turning off their personal mobile phones during class hours. • If the employees (teacher, administrator, staff, etc.) act against the school policy, disciplinary action is initiated. • Employees of the institution (teachers, administrators, staff, etc.) and students bear the legal responsibility of any content and messaging that will come from or send by students or institution employees via social media or chat programs, any content and messaging that may be inappropriate immediately. shared with. Necessary precautions are taken to prevent such a situation.

ONLINE EVENTS AND PROTECTION:
• All members of our school will be informed about online risks.
• In our school, information activities are carried out on issues such as illegal content, security breach, cyber bullying, sexual messaging, child abuse, and personal information security.
• Awareness is tried to be raised by organizing various events on the safe internet day.

• All complaints about the misuse of internet, information technologies and equipment in our school will be reported to the school principal.
• All members of our school are informed to act in accordance with official school rules in order to eliminate privacy and security concerns.
• The school is responsible for taking necessary actions in case of negativity.
• Employees (teachers, administrators, staff, etc.), parents and students should act together with the school to solve the problems.

Kazım Dönmez y.
School Principal