Gül Çetin Kaur Anatolian High School

e-Safety (e-Safety) POLICY

and

OBJECTIVES

As Gül Çetin Kaur Anatolian High School, in line with the circular numbered 2018/10 of the Ministry of National Education support services general directorate on "Taking Security Measures in Schools"; security policy file has been prepared. The school policy was determined based on the themes of life safety, internet safety and personal safety at the school. The school security policy is evaluated as a requirement of the 2018/2023 strategic plan and all necessary e-security measures are taken.

With the rapid development of technology, it has become inevitable for every school to have a School Security Policy. Because stakeholders can access the internet in a variety of ways from the school building today. As a part of our daily lives, we all live with digital technologies. To ensure that our children know how to best use the opportunities available through digital technologies, it is now necessary to know and understand how to use them. To ensure this is done in the safest and most secure environment possible, we are a school with a clear and concise Safe Internet School Policy that grabs the attention of our students when they are at home, at school or outside, with friends or alone.

A. OUR E-SAFETY POLICY IN SUMMARY:

1. Our school has a website and social networks such as facebook. The data published on these networks is shared in a controlled manner.

2. In our school, mobile phones are kept off during the lesson, and friends who make eTwinning projects use them for project work if necessary.

3. Seminars on ICT addiction, correct and safe use of ICT, and Cyber Bullying are organized regularly by our teachers. We have teachers with certificates on this subject.

4. There are fixed boards in our school regarding the correct and safe use of ICT.

5. Some teachers of our school received remote and face-to-face training on Cyberbullying and the correct and safe use of ICT, given by the Ministry of National Education.

6. "Safer Internet Day" is celebrated in our school.

7. On the subject of e-security on our school's website, safeweb.org.tr. website link. Our school stakeholders can get information about the subject whenever they want.

8. Safe internet day celebrations in our school, seminars on the subject,safeweb.org.tr. Information brochures quoted from the website are distributed.

9. Our 9th Grade Teachers convey their knowledge about internet ethics and safe internet use to our students.

10. 21st century communication skills are considered important in our school. In this regard, efforts are being made to improve our students' ICT usage skills.

11. In our school, awareness raising activities are carried out for our stakeholders about being a digital citizen.

12. The internet provider (MEB) at the school has blocked access to all kinds of harmful content. Access to these sites is blocked by the MEB internet filtering network.

13. Ministry of National Education General Directorate of Legal Services, according to the article dated 07.03.2017 and numbered 2975829 and numbered 2017-12 on Use of Social Media in Schools, taking and publishing photos of students, parents and staff is prohibited for security reasons.

14. By adjusting the privacy and security settings of the browsers, cyberbullying is prevented by using a virus program.

15. Necessary precautions are taken to prevent the use of mobile devices/mobile phones other than for educational purposes.

B. PURPOSE OF E-SECURITY POLICY AT OUR SCHOOL;

• To protect and secure all members of our School online.

• To raise awareness for Gül Çetin Kaur Anatolian High School administrators, teachers, students and employees about the potential risks and benefits of technology.

• Ensuring that all personnel 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.

• This policy applies to all personnel, including the governing body, teachers, support staff, external contractors, visitors, volunteers, and others who provide or perform services on behalf of the school (collectively referred to as 'staff' in this policy), as well as ensure that it includes children and parents,

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.

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.

THE MAIN RESPONSIBILITIES OF CHILDREN AND YOUTH ARE THE FOLLOWING:

• 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.

•

THE 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.

Managing the 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.

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 parents will always be obtained before the electronic publication of students' pictures / videos.

Video Conferencing Rules

• Students will seek a teacher's permission before preparing or answering a video conference call or message.

• Video conferencing will be moderated appropriately for students' age and ability.

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

• Videoconferencing will take place through formal and approved communication channels, following a sound risk assessment.

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

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

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 cell phones and other personal devices by teenagers and adults will be decided by the school and included in appropriate policies, including the school Acceptable Use or Cell Phone Policy.

• Gül Çetin Kaur Anatolian High 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.

Students' use of personal devices and mobile 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.

Visitors use of personal devices and mobile phones

• Parents and visitors must 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.

Participation and education of children and young people

• An online safety (e-Safety) curriculum is created and included throughout the school to raise awareness among students about the importance of safe and responsible internet use.

• Training on safe and responsible use will be given before internet access.

• Student input will be sought when writing and developing school online safety policies and practices, including curriculum development and enforcement.

• Students will be supported to read and understand the Acceptable Use Policy in a manner appropriate to their age and ability.

• All users will be notified that their network and internet usage will be monitored.

• Acceptable Use expectations and Posters will be posted in all rooms with Internet access.

• Safe and responsible use of internet and technology will be strengthened in the curriculum and in all subjects.

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

• The school will reward students for using technology in a positive way.

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

Involvement and training of staff

• The online safety (e-Safety) policy will be formally provided and discussed for the participation of all employees and will be strengthened and emphasized as part of our responsibility to protect.

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

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

• All members of staff will realize that their online behavior can affect their role and reputation in the school. Public, disciplinary or legal action may be taken if something is thought to have put the profession or organization in a state of decay or has lost confidence in their professional abilities.

• Members of staff responsible for managing filtration systems or monitoring ICT usage 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 students' ages and abilities.

Parent involvement and education

• Gül Çetin Kaur Anatolian High School recognizes that parents have an important role to play so that children can become reliable and responsible users of the internet and digital technology.

• Parents' attention will be directed to the school online safety (e-Safety) policy and expectations on the school disclosures and school website.

• As part of our school, parents will be required to read online safety information.

• Parents will be encouraged to read the School Acceptable Use Policy and discuss its implications with their children.

• Information and guidance for parents on online safety will be available to parents in a variety of formats.

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

Responding to Online Incidents and Protection issues

• All members of the school, objectionable messaging, online / cyberbullying, etc. will be made aware of the variety of online risks that may be encountered, including This will be emphasized in staff training and training approaches for students.

• All members of the school are subject to filtering, objectionable messaging, cyberbullying, illegal content violation, etc. will be informed of the procedure for reporting online security (e-Security) concerns, such as

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

• Complaints about misuse of the Internet will be handled under the school's grievance procedures.

• Online/cyberbullying related complaints will be handled under the school's anti-bullying policy and procedure.

• Any complaint about staff misuse will be directed to the school principal.

• School grievance procedure will be communicated to students, parents and staff.

• Complaint and notification procedure will be notified to the personnel.

• All members of the school should be aware of the importance of confidentiality and the need to follow official school procedures for reporting concerns.

• All members of the school will be reminded of safe and appropriate behavior online and reminded of the importance of not posting any content, comments, pictures or videos that cause harm, distress or offense to any other member of the school community.

• The school manages online safety (eSafety) incidents in accordance with the school discipline / behavior policy, where appropriate.

• The school notifies parents of their concerns when needed.

• After any investigation is complete, the school will receive information, identify lessons learned and implement changes as needed.

• Parents and children need to work in partnership with the school to solve problems.

Bulent YILMAZ

Signature

Seal