

Cumhuriyet Primary School e-Security Policy

Objectives and Policy Scope

- Cumhuriyet Primary School believes that online security (eSecurity) is an indispensable element for the protection of children and adults in the digital world while using technology such as computers, tablets, mobile phones or game consoles.
- Cumhuriyet Primary School believes that the Internet and information communication technologies are an important part of everyday life. Therefore, children should be supported to manage risks and learn ways to develop strategies to respond to them.
- Cumhuriyet Primary School has an obligation to provide quality Internet access to the community in to raise educational standards, promote success, support the professional work of staff and improve management functions.
- Cumhuriyet Primary School is responsible for protecting all children and staff from potential harm online.
- This policy is for administrators, teachers, support staff, children and parents.
- This policy applies to the use of information communication devices, including internet access and personal devices; Remote use of children, staff or others, such as laptops, tablets or mobile devices where they work, also applies to devices issued by the Turkey school.

The responsibilities of all employees are:

- Contribute to the development of online security policies.
- Read and stick to acceptable usage policies.
- To be responsible for the security of school systems and data.
- To have awareness of a number of different online safety and to know how they can be associated with children in their care.
- Modeling good practices when new and emerging technologies are used.
- Associate online safety training with curriculum as much as possible.
- To identify and take precautions against concerned individuals by following school protection policies and procedures.
- To emphasize positive learning opportunities.
- To take personal responsibility for professional development in this field.

The main responsibilities of children are:

- Contribute and comply with the development of online security policies.
- Learn and stick to the School's Acceptable Use Policies.
- Respect the feelings and rights of others online and offline.
- If things go wrong, ask a trusted adult for help and support others who are having online security issues.
- To be responsible for their own awareness and learning about the opportunities and risks of new and emerging technologies.
- To be safe and responsible to assess and limit the personal risks of using certain technology.

The main responsibilities of parents are:

- To read the School Acceptable Use Policies, to encourage their children to stick to it, and to ensure that they remain as committed as possible.
- Discussing online safety issues with 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.
- Asking the school or other appropriate institutions for help or support if they or their children encounter problems or problems online.
- Contributing to the creation of the school's online security policies.

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 Principal will take responsibility for the general publication of published online content and ensure that the information is accurate and appropriate.
- The website will follow the school's editorial guidelines, including respect for accessibility intellectual property rights, privacy policies and copyright.
- To protect against spam, email addresses will be published carefully online.
- Student studies will be published with the permission of the students or with the permission of their parents. •The administrator account of the school website will be protected by encrypting it with an appropriately strong password.

- The school will post information about protection on the school website for members of the community, including online safety.

Convenient and secure 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 training to support and assist them in developing strategies to respond to their problems as part of the integrated school curriculum.
- Teachers and students can only use the Internet network controlled by the Ministry of National Education at the school.
- Our school can not connect to the internet network without the download of the MEB CERTIFICATE security file.
- Only teachers' registered devices are used, even if they are for the project within the school.
- Communication and video communication with other project partners is carried out by teachers during school hours.
- Our e-security policy is included in the secure internet framework issued by the Ministry of National Education. (Ministry of National Education Circular No. 2017/12)
- All members of employees are aware that they will not rely on filtering alone to protect children, and supervision, classroom management and safe and responsible use training are important.
- All school-owned devices will be used in accordance with the school's Acceptable Use Policy and by taking appropriate safety and security measures.
- Staff members will always evaluate websites, tools and applications before using them in the classroom or when recommending using them at home.
- The school will ensure that the materials derived from the Internet by staff and students comply with copyright laws and accept sources of information.
- Students will be taught to think critically before accepting the accuracy of the information they have learned or shown.

Use of Personal Devices and Mobile Phones

Students' use of personal devices and mobile phones:

- Our students will not bring mobile phones, tablets and computers to school because they are at primary school level as of age.
- Students can use the school's internet and computer for projects and studies. The use is done by checking the filtering by taking e-security measures under the supervision of the teacher on duty.

Staff's use of personal devices and mobile phones

- Staff will always provide data protection and the fulfillment of any use of personal phones and devices in accordance with relevant school policies and procedures.
- Personal mobile phones and devices are turned off during class hours and put into silent fashion.
- Bluetooth or other forms of communication must be "hidden" or turned off during lesson hours.
- Disciplinary action is carried out if a staff member violates school policy.
- If a member of staff has illegal content recorded or stored on a mobile phone or personal device, or has committed a criminal offense, the police will be contacted.
- Any claim involving staff using their mobile phone or devices personally will be responded to by following the school administration policy.

Visitors use personal devices and mobile phones

- Parents and visitors must use their mobile phones and personal devices in accordance with the school's acceptable use policy.
- It is not acceptable for visitors and parents to take photos or videos of students within the school. Therefore, the necessary warnings are made.

Participation and education of children

- Student contributions will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Students will be supported to understand the Acceptable Use Policy in accordance with their age and abilities.
- All users will be notified that network and internet usage will be monitored.

- Acceptable Usage expectations and Posters will be published 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.
- The school will reward students for their positive use of technology.
- Safe Internet Day is celebrated in our school. Within the framework of Safe Internet Day, presentations are made in classrooms in the first week of February and videos are watched. Via Eba
<http://www.eba.gov.tr/video/izle/9811b430f368c4d6c436e838384acaf94fd729813a002> information security is monitored in the public spotlight.

Participation and training of personnel

- The online safety (e-Security) policy will be formally provided and discussed for the participation of all employees and will be strengthened and emphasized as part of our protection responsibility.
- Our school staff will be informed about our school's e-security policy during the teachers' board meetings held during the year. E-security policy will be developed by exchange of views.
- The e-security policy of our school will be discussed in the meetings of the board of teachers of the clan between the teachers who are studying the same class in our school.
- Staff will be aware that Internet traffic can be monitored and monitored up to a single user. Discretion and professional conduct are required when using school systems and devices.
- Up-to-date and appropriate personnel training on safe and responsible Internet use will be provided to all members of staff professionally and personally in a variety of ways on a regular (at least annual) basis.

Participation and education of parents

- Cumhuriyet Primary School accepts that parents have an important role to play in order for children to become reliable and responsible users of the Internet and digital technology.
- Parents' attention will turn to school online safety (e-Security) policy and expectations on school descriptions and the school website.
- Information and guidance for parents on online safety will be available to parents in a variety of ways. E-security and parents information meetings will be held and the necessary information and opinions will be exchanged by taking as e-security agenda items in school general parents meetings and class parents meetings.

- Parents will be encouraged to role model positive behaviors for their children within the scope of esecurity.

Respond to Online Events and Protection issues

- All members of the school will be informed of the variety of online risks that may be encountered,including sexually explicit messaging, online/cyberbullying, etc. This will be emphasized in personnel training and training approaches for students.
- All members of the school will be notified of the procedure for reporting online security (e-Security) concerns such as filtering, sexually explicit messaging, cyberbullying, illegal content violations, etc.
- The Digital Subscriber Line (DSL) will be notified of any online safety (e-Security) incident involving child protection concerns that will be recorded later.
- Complaints about the mis-use of the Internet will be dealt with within the scope of the school's complaints procedures.
- Complaints about online/ cyberbullying will be dealt with within the scope of the school's anti bullying policy and procedure.
- Any complaints about misunderstood personnel will be directed to the headmaster
- The school complaints procedure will be reported to students, parents and staff.
- Complaints and notice procedures will be reported to the staff.
- All members of the school should be aware of the importance of privacy and the need to comply with official school procedures to report concerns.
- All members of the school will be reminded of safe and appropriate behaviour online and will be reminded of the importance of not publishing any content, comments, pictures or videos that cause harm, distress or criminality to any other member of the school community.
- The school manages online safety (e-Safety) incidents, where appropriate, in accordance with the school discipline/conduct policy.
- The school informs parents of concerns about them when they are needed.
- After any investigation is completed, the school will receive information, determine the lessons learned and implement the changes as needed.
- Parents and children need to work with the school to solve problems.