Akdere Şehit Öğretmen Hamit Sütmen Secondary School e-Security Policy

Akdere Ş.Ö.H.S. Scondary School e-Security Policy

Objectives and Policy Scope:

• Akdere Ş.Ö.H.S.S.Sbelieves that online security (e-Security) is an indispensable element in order to protect students while using digital devices such as computers, tablets, mobile phones or game consoles.

• Akdere Ş.Ö.H.S.S.S believes that internet and information communication technologies are an important part of daily life. Therefore, children should be supported to develop strategies against risks.

• Akdere Ş.Ö.H.S.S.S is obliged to raise the standards of education, to promote success, to support the professional work of the personnel and to provide quality internet access to improve the management functions.

• Akdere Ş.Ö.H.S.S.S is responsible for ensuring that all students are protected from potential damage to the digital environment.

• All members of the school are involved in sexual messaging, cyber bullying, etc. including online risks.

• All members of the school are informed about reporting online security (e-Security) issues such as filtering, sexual messaging, cyber bullying, and illegal content infringement.

• This policy is intended for administrators, teachers, support staff, students and parents.

• This policy also applies to laptops, tablets, or mobile devices provided to students or staff by the school, including personal devices with internet access.

The responsibilities of all employees are:

• Contribute to the development of online security policies.

• Read and adhere to Acceptable Use Policies.

• Be responsible for the security of school systems and data.

• To learn good practices using new and emerging technologies.

• Associate curriculum and online safety training as much as possible.

• Identify and take action by monitoring school protection policies and procedures.

- Emphasis on positive learning opportunities.

- To take personal responsibility for professional development in this field.

The main responsibilities of the students are:

- Contribute to the development of online security policies.

- Read and adhere to the School's Acceptable Use Policies.

- Respect the feelings and rights of others, online and offline.

- If things go wrong, ask for help from a trusted adult and support others who are experiencing online security issues.

- Take responsibility to protect themselves and others online.

- To know the opportunities and risks of new and developing technologies

- Knowing the personal risks of using technology.

The main responsibilities of the parents are:

- Reading School Acceptable Use Policies, encouraging children to adhere to this policy and ensuring that they adhere to them as appropriate.

- Discuss online safety issues with their children, support the school's online safety approaches, and reinforce appropriate safe online behavior at home.

- Modeling the safe and appropriate use of technology and social media.

- Identify changes in behavior that indicate that the child is at risk of harm online.

- Seek help or support from the school or other appropriate institution if they or their children encounter problems or problems online.

- Contribute to the creation of the school's online security policies.

- Safe and appropriate use of school systems such as learning platforms and other network resources.

• To be responsible for their own awareness and learning about the opportunities and risks of new and emerging technologies.

Safer Use of Online Communication and Technology Managing the school / website:

• The contact details on the website will be the school address, e-mail and telephone number. Personal information of staff or students will not be published.

• The Principal will assume the overall publication responsibility for the published online content 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.

• To protect against spam emails, email addresses will be published online carefully.

• 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 being properly encrypted with a strong password.

• The school will send information about protection on the school website to members of the community, including online security.

Publish images and videos online:

• The school will ensure that all pictures and videos shared online are used in accordance with the school's online security (e-Security) policy.

• The use of images and videos in the school will be carried out 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 online security (e-Security) policy, parents 'written consent will always be obtained prior to electronic publication of students' pictures / videos.

• Students will ask a teacher for permission before preparing or replying to a video conference call or message.

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

• Parents' consent will be obtained before children participate in video conferencing activities.

• Video conference will take place through formal and approved communication channels following a sound risk assessment

- Only master managers will be granted access to the video conference management areas or remote control pages.

- Private login and password information for educational videoconferencing services will only be provided to personnel and kept confidential.

Convenient and safe use of the Internet and related devices:

- The use of the Internet is an important feature of educational access and all children will receive appropriate age and ability to support and assist them in developing strategies to address their problems as part of the integrated school curriculum.

- The school's Internet access will be designed to develop and expand education.

- Internet access levels will be reviewed to reflect curriculum requirements and students' age and abilities.

- All members of employees are aware that they do not rely on filtering alone to protect children, and supervision, classroom management and safe and responsible use training are important.

- All school equipment will be used in accordance with the school's Acceptable Use Policy and appropriate safety and security measures.

- Staff will always evaluate websites, tools, and applications before using them in the classroom or when suggesting to use them at home.

- Students will be trained on the effective use of information in research on the Internet, including skills in positioning, retrieving, and evaluating information.

- The school will ensure that staff and students comply with the copyright laws of materials derived from the Internet and accept their sources of information.

- Students will be taught to think critically before accepting the accuracy of the information they have read or shown.

- Evaluation of online materials is part of teaching and learning in all subjects and is seen as a whole in the curriculum.

- The school will use the Internet to enable students and staff to communicate and collaborate in a safe and confidential environment.

Use of Personal Devices and Mobile Phones:

- Our school is obliged to make the necessary arrangements to ensure that children use their mobile phones and other personal devices responsibly.

- The use of mobile phones and other personal devices of adults in our school will be provided in accordance with the Mobile Phone Use Policy rules set by the school.

- Our school is aware that personal communication with mobile technologies is an accepted part of everyday life for children, staff and parents; however, it must take the necessary measures to ensure the safe and proper use of such technologies in the school.

- Use of personal devices and mobile phones will be carried out in accordance with the law and other appropriate school policies.

- The user is responsible for all electronic devices brought to the school. The school assumes no responsibility for the loss, theft or damage of such devices.

- The school assumes no responsibility for any adverse health problems caused by such devices.

- Disciplinary policy rules apply if abuse, inappropriate messages or content is sent with these devices.

- All members of the school are advised to take the necessary measures to protect their mobile phones or devices from loss, theft and damage.

- All members of the school are advised to use a password to prevent unauthorized calls to their phones or devices if they are lost or stolen.

- All members of the school are advised to ensure that their mobile phones and personal devices do not contain any content that is offensive, scornful or otherwise contrary to school policies.

Students use personal devices and mobile phones:

- Students will be trained in the safe and proper use of personal devices and mobile phones.

- All use of children's mobile phones and personal devices will be in accordance with an acceptable use policy.

- Mobile phones or personal devices may not be used by students during lectures or formal school hours unless they are approved and approved by a faculty member and are not covered by a curriculum-based activity.

- The use of children's mobile phones or personal devices at the educational event will only take place when approved by the school administration.

- When a student needs to call their parents, they will be allowed to use the school phone.

• Parents should not communicate with their children by mobile phone during school hours with the permission of the school administration.

• Students should give their phone numbers only to trusted friends and family members.

• Students will be taught the safe and proper use of mobile phones and personal devices, and the limits and consequences will be recognized.

• If the material on the student's personal device or mobile phone is suspected to be illegal or provide evidence of a criminal offense, the device is delivered to the police for further investigation.

Personnel use of personal devices and mobile phones

Staff do not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children. It only uses devices provided by the school.

• Personal cell phones and devices of the personnel are switched off during class hours or switched to silent mode.

• Bluetooth or other forms of communication must be "hidden" or turned off during class hours.

• In case of emergency, personal mobile phones or devices may not be used during the school period unless authorized by the school administration.

• Disciplinary action is taken if a staff member violates school policy.

• Security personnel will be notified if a personnel has illegal content recorded or stored on a mobile phone or personal device, or has committed a criminal offense.

• Any claim involving personal use of staff's mobile phones or devices will be responded to by following the school management policy.

Participation and education of students:

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

• Training on safe and responsible use will take place prior to internet access.

• Student contributions will be sought when writing and developing school online security policies and practices, including curriculum development and implementation.

• Students will be supported to read and understand the Acceptable Use Policy in accordance with their age and abilities.

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

• Online security (e-Security) will be included in PSHE, SRE, Citizenshipand Computing / ICT programs and will cover both safe school and home use.

• Acceptable Use 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 matters.

• External support will be used to complement and support schools' internal online security (e-Security) training approaches.

• The school will reward students for their positive use of technology.

• The school will implement peer education to improve online safety in accordance with the needs of the students.

Staff involvement and training:

• Online security (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.

• Personnel will be aware that Internet traffic can be tracked to a single user.

• Up-to-date and appropriate staff training on safe and responsible Internet use will be provided to all members of staff on a regular basis (at least annually).

• Staff will realize that their online behavior can affect the reputation of the school.

• Personnel responsible for managing filtration systems or monitoring ICT use will be supervised by the school management.

• The school will provide useful online tools that employees must use according to the age and ability of the students.

Parental involvement and education:

• Akdere Ş.Ö.H.S.S.S recognizes that parents have an important role to play in ensuring that children can be trusted and responsible users of the Internet and digital technology.

• Parents' attention will be directed to school online security (e-Security) policy and expectations on the school descriptions and school website.

• As part of the School Agreement, parents will be asked to read online safety information.

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

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

Responding to Online Events and Protection issues:

• All members online, sexual messaging, online / cyber bullying, etc. Be aware of the variety of online risks that may occur, including

• All members of the class, filtering, sexual content messaging, cyber bullying, illegal content violation, and so on. online security (e-Security) concerns.

• Complaints about misuse of the Internet, examination of the school's complaints procedures will be addressed.

• Complaints about online / cyber bullying will be addressed, review the school's anti-bullying terms and procedure

• Any complaints about misuse of staff in school management

• The school will notify the students, parents and staff about the grievance procedure.

• Inform the personnel of the complaint and notice procedure.

• All official members are aware of the importance of confidentiality and the need to follow formal school procedures to report concerns.

• All groups will be reminded of the safe and appropriate behavior of online use and will remind the school community of the importance of not harming any other membership, experiencing hardship or criminal content, comments, images or videos.

• The school manages online security (e-Security) incidents in accordance with the school discipline / behavior policy, as appropriate.

• The school notifies parents of any concerns you may need.

• After completing any application, the school will receive information, identify lessons learned and use.

• Parents and students need to collaborate with the school to solve problems.