**NECMI ŞAHİN PRIMARY SCHOOL E-SECURITY POLICY**

**Objectives and Policy Scope**

* Necmi Şahin Primary School believes that online security (e-Security) is an indispensable element for the protection of children and adults in the digital world when using technology such as computers, tablets, mobile phones or game consoles.
* Necmi Şahin Primary School believes that the internet and information and communication technologies are an important part of daily life. Therefore, children should be supported to learn ways to manage risks and develop strategies to respond to them.
* Necmi Şahin Primary School has the obligation to provide the society with quality Internet access in order to raise educational standards, encourage success, support the professional work of personnel and improve management functions.
* Necmi Şahin Primary School is responsible for ensuring that all children and personnel are protected from potential harm online.
* This policy is intended for administrators, teachers, support staff, children and parents.
* This policy applies to internet access and use of information communication devices, including personal devices; This also applies to school-issued devices for remote use by children, staff or others, such as laptops, tablets or mobile devices where they work.

**The responsibilities of all employees are:**

* Contribute to the development of online security policies.
* Read and adhere to the Acceptable Use Policies.
* 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 the curriculum with online safety training.
* Identifying individuals who are concerned and taking 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 are:**

* 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.
* 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 certain technology.

**The main responsibilities of parents are:**

* Read the School's Acceptable Use Policies, encourage their children to adhere to this policy, and ensure that they do, as appropriate.
* Discussing online safety issues with their 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.
* Identifying changes in their 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.
* Contribute to the creation of the school's online safety policies.
* Using school systems, such as learning platforms and other network resources, safely and appropriately.
* Be 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, email 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 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 compliance 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, official written permission from the parents will always be obtained before the electronic publication of the images / videos of the students.

**Formal video conferencing and webcam use for educational purposes**

* The school recognizes that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential for the entire activity.
* All video conferencing equipment will be turned off when not in use and available, not set to auto answer.
* External IP addresses will not be made available to other sites.
* Video conference contact details will not be shared publicly.
* Video conferencing equipment will be kept securely and, if necessary, locked when not in use.
* School video conferencing equipment will not be removed from school buildings without permission.
* Staff will ensure that external video conferencing opportunities and/or tools are appropriately evaluated and that the accounts and systems used to access events are appropriately secure and confidential.

**Users**

* 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.
* The 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.

**Contents**

* When recording a video conference lecture, written permission will be obtained from all sites and participants. The reason for registration should be stated at the beginning of the conference and the video conference recording should be open to all parties. Recorded materials will be stored securely.
* If third party materials are to be included, the school will check that recording is acceptable to avoid violating the third party's intellectual property rights.
* The school will engage in dialogue with other conference participants before participating in a video conference. If not, the school will check that it has received material suitable for the class.

**Appropriate and safe use of the Internet and related devices**

* Internet use is an important feature of educational access and all children will receive age- and ability-appropriate education that will support and assist them in developing strategies to answer their problems as part of the integrated school curriculum. Please access specific curriculum policies for more information.
* The school's internet access will be designed to improve and expand education.
* Internet access levels will be reviewed to reflect curriculum requirements and students' age and abilities.
* All members of staff are aware that they cannot rely on filtering alone to protect children, and training for supervision, classroom management and safe and responsible use is important.
* It will be appropriate for the ages and abilities of the students.
* All school-owned devices will be used in accordance with the school's Acceptable Use Policy and with appropriate safety and security measures.
* Staff members will always evaluate websites, tools, and apps before using them in the classroom or when suggesting to use them at home.
* Students will be trained in the effective use of Internet research, including the skills to locate, retrieve and evaluate information.
* The school will ensure that staff and students accept materials derived from the Internet and comply with copyright laws.
* 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 in the curriculum as a whole.
* The school will use the internet to enable its students and staff to communicate and collaborate in a secure and confidential environment.

**Use of Personal Devices and Cell Phones**

* Widespread ownership of mobile phones and other personal devices among children, teenagers 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.
* Necmi Şahin Primary 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.

**Expectations for the safe use of personal devices and mobile phones**

* Use of personal devices and mobile phones will be conducted in accordance with the law and other appropriate school policies.
* The responsibility of any electronic device brought to the site belongs to the user. The school accepts no responsibility for the loss, theft or damage of such items. The school accepts no responsibility for any potential or actual adverse health effects caused by such devices.
* Abuse or sending inappropriate messages or content via mobile phones or personal devices is prohibited by any member of the community and any violation will be treated as part of the discipline/behavior policy.
* All members of the Necmi Şahin Primary School community are encouraged to take steps to protect their mobile phones or devices from loss, theft or damage.
* All members of the Necmi Şahin Primary School community are advised to use passwords / pin numbers to ensure that unauthorized calls or movements cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers must be kept confidential. Cell phones and personal devices should not be shared.
* All members of the Necmi Şahin Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content that is offensive, disparaging or otherwise inconsistent with school/setting policies.

**Student use of personal devices and mobile phones**

* Students will be trained in the safe and appropriate use of personal devices and mobile phones.
* All use of mobile phones and personal devices by children will be restricted in accordance with their age.
* Cell phones or personal devices may not be brought to school by students during classes or official school hours unless they are part of an approved and directed curriculum-based activity with the approval of a faculty member.
* 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.
* Students should only give their phone number to trusted friends and family members.
* Students will be taught the safe and appropriate use of mobile phones and personal devices, and will recognize the limitations and consequences.
* If it is suspected that material found 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.

**Staff use of personal devices and mobile phones**

* Staff are not allowed to connect their personal phones or devices with children, young people and their families in or outside the setting in a professional capacity. Any pre-existing relationships that would endanger this issue will be discussed with managers.
* Staff do not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and only use business-provided equipment for this purpose.
* Staff do not use any personal devices directly with children and only use school-provided equipment during lesson/educational activities.
* Staff will ensure that any use of personal phones and devices is always carried out in accordance with data protection and relevant school policy and procedures.
* Staff personal mobile phones and devices are turned off / put into silent mode during class hours.
* Bluetooth or other forms of communication must be "hidden" or turned off during class hours.
* Personal mobile phones or devices cannot be used during teaching periods unless authorized by the school administration in emergencies.
* The staff will ensure that the content purchased on the site via mobile phones and personal devices is compatible with their professional role and expectations.
* Disciplinary action is taken when a staff member violates school policy.
* Police will be contacted if a staff member has illegal content recorded or stored on a mobile phone or personal device or has committed a criminal offence.
* Any claim involving staff's personal use of mobile phones or devices will be responded to by following school administration policy.

**Education of children**

* 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 contributions 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 network and internet usage will be monitored.
* Online security (e-Security) will be included in PSHE, SRE, Citizenship and Computing / ICT programs and will cover both safe school and home use.
* Acceptable Use expectations and Posters will be posted 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.
* External support will be used to complement and support schools' internal online safety (e-Safety) 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.
* Safer internet day (SID) will be celebrated at school and information about safe internet will be given with activities to be held.

**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 highlighted 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.

**Education of parents**

* Necmi Şahin Primary 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's online safety (e-Safety) policy and expectations on the school disclosures and school website.
* As part of the School Agreement, parents will be required to read the 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 are encouraged to role model positive behavior for their children online.

**Responding to Online Incidents and Protection issues**

* All members of the school, 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, 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, which will be recorded later.
* Complaints about misuse of the Internet will be handled under the school's complaints procedures.
* Complaints about online/cyberbullying will be handled under the school's anti-bullying policy and procedure
* Any complaint regarding the misuse of staff 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 (e-Safety) incidents in accordance with the school discipline/behavior policy, where appropriate.
* The school notifies parents of concerns about these 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.

Eset ÖZÜGÜZEL

School Principal