**T.C.**

**MİLLÎ EĞİTİM BAKANLIĞI**

**Sarıçam Kaymakamlığı**

**Sevgi Anaokulu Müdürlüğü**

School eSafety Policy

SEVGİ KINDERGARTEN

**Adana, 2021**

**Development / Monitoring / Review of this Policy**

This e-safety policy has been developed for “Sevgi Kindergarten” Working group: , Emine ÖZDEMİR, Recep GÜZELEL, Fatma GÜRSOY, Elif KONAKLI. Schools will need to agree the content of this document with staff and amend sections where necessary.

**Scope of the Policy**

This policy applies to all members of Adana “Sevgi Kindergarten” (including staff, students / pupils, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of school. There should be an incident of cyber bullying covered by this policy, which may take place out of school, but is linked to membership of the school, the headteacher can impose disciplinary penalties for inappropriate behaviour where this is reasonable.

**Roles and Responsibilities**

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school: Headteacher :

• The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community

• The Headteacher will appoint a designated person as E Safety Coordinator for the school. This will usually be the School’s Child Protection Officer.

• The Headteacher will receive regular monitoring reports from the E-Safety Co-ordinator

• The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

 • The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable them to carry out their esafety roles and to train other colleagues, as relevant

**ESafety Coordinator :**

The security coordinator of Sevgi Kindergarten is responsible for following the specified works.

• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents

• Ensures that all staff are aware of the procedures that need to be followed in the event of an esafety incident taking place.

• Provides training and advice for staff

• Receives reports of e-safety incidents and records them on agreed reporting format to inform future

• Reports regularly to Senior Leadership Team

• They should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

\* Sharing of personal data o access to illegal / inappropriate materials

\*İnappropriate on-line contact with adults / strangers

\* Potential or actual incidents of grooming Cyber-bullying

**Teaching and Support Staff ,**

are responsible for ensuring that:

• they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices

• they have read and understood the school Staff AUP a copy of which is available, displayed in each staff room.

• they report any suspected misuse or problem to the E-Safety Co-ordinator

• digital communications with students / pupils (email / Virtual Learning Environment / voice) should be on a professional level and only carried out using official school systems.

• e-safety issues are embedded in all aspects of the curriculum and other school activities

• students / pupils understand and follow the school e-safety

• students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• they monitor ICT activity in lessons, extra curricular and extended school activities

• they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

• in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

**Students / pupils:**

• Contribute to the development of online security policies.

• Understand and adhere to the School's Acceptable Use Policies.

• Respecting the feelings and rights of others online and offline.

• Seek help from a trusted adult if things go wrong.

• At a level appropriate for their age, abilities and weaknesses:

* Taking responsibility for protecting themselves online.
* Being aware of the opportunities and risks brought by new and emerging technologies.
* Knowing the personal risks of using a particular technology.

**Parents**

* Read the School's Acceptable Use Policies, encourage their children to adhere to this policy, and ensure that they do so 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.
* Model 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.
* Seeking help or support from the school or other appropriate agency if they or their children encounter problems or problems online.
* Contributing to the creation of the school's online safety policies.
* Using school systems, such as learning platforms and other network resources, safely and appropriately.
* Being responsible for their own awareness and learning regarding the opportunities and risks posed by new and emerging technologies.

**BASIC PRINCIPLES**

**Terms of Use**

By using the School's computer systems, all users agree that the School makes no representations about the confidentiality of any messages or data stored in or sent through such systems; They accept that the School reserves the rights specified in this document and that the use of the said systems is limited to the School-approved purposes, and that the necessary notifications have been made to them. The use of the School's computer systems in connection with the School's activities and personal use of minor matters is not a right, but It is a privilege granted to limited members of the school community. Therefore, the School may at any time and without notice block access to all or part of its computer systems (for all or some users) in whole or in part. Users of the School's computer systems must comply with the Sevgi Kindergarten's Acceptable Use Policy, and that they have accepted and will abide by the Acceptable Use Policy by using the said systems, that they have been notified in this regard and that the School's Acceptable Use Policy They accept that they have given permission to apply the Users also agree that they will comply with the relevant legislation and refrain from any behavior that will put the School under liability. The School reserves the right to change the Sevgi Kindergarten Acceptable Use Policy and other conditions regarding the use of computer systems at any time without prior notice, and to take actions that are required or appropriate to be taken in accordance with the relevant legislation. To protect the integrity of the School, the School's computer systems and its users against unauthorized or improper use of the facilities in question, and to identify possible uses that may result in violation or violation of the School's rules and policies; reserves the right to limit or prevent any person's use without notice, and to search, copy, remove or modify any data, file or system resource that may harm the appropriate use of a computer system or be used in violation of the School's rules or policies. . Sevgi Kindergarten reserves the rights of periodic control of the systems and all other rights for the protection of computer systems. Malware scanning systems in e-mail messages processed on computers, smart boards, servers, and school servers are examples of controls for protection purposes.The school is not responsible for the work it will carry out to ensure the confidentiality and security of the systems in question, data loss that may occur due to system malfunction or any other reason, or interference with files.

**A.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 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.

**B.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 prior to electronic publication of students' pictures/videos.

**C.USE OF PERSONAL DEVICES AND MOBILE 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 mobile phones and other personal devices by children, teenagers and adults will be decided by the school and will be covered in appropriate policies, including the school Acceptable Use or Cell Phone Policy.
* Sevgi Kindergarten 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.

**D.USE OF STUDENTS' PERSONAL DEVICES AND MOBILE PHONES**

* No student will be allowed to enter the school with a mobile phone.
* 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 mobile phones or personal devices by children in the educational activity will take place when approved by the school administration.
* The school phone will be used when students need to communicate with their parents.
* Parents are advised not to communicate with their children on cell phones during school hours and to apply to the school administration. Exceptions may be permitted in exceptional circumstances as approved by the teacher.
* Students will be taught the safe and appropriate use of mobile phones and personal devices, and will be encouraged to be aware of their limitations and consequences.
* The rules for children will be determined together with their parents and teachers, enough work will be done so that all students can understand the rules.

**E. USE OF VISITOR 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 of their usage prospects.
* Staff are expected to oppose problems when appropriate and safe and will always report any violations by visitors to the administration.

**METHOD**

**Acceptable Use Policy**

Sevgi Kindergarten shares its computer systems with its administrators and teachers. These systems should be used with caution; Even the misuse of a few people has the potential to disrupt the work of the School and others.

For this reason, users should be careful and behave ethically when using the School's computer systems. This obligation includes, but is not limited to:

* Users may not copy, modify, reproduce, create derivative works from, reverse engineer, disassemble,

or otherwise decompile any software or other part of computer systems.

* Users cannot use computer systems that the School does not allow. Unauthorized use of computer systems by providing false or deceptive information or otherwise in order to gain access to computer systems is prohiICTed. Users may not use the School's computer systems to gain unauthorized access to the computer systems of other institutions, organizations or individuals.
* Users may not authorize anyone for any reason to use their School account. The account holder is responsible for any use of the school account. Users should take all reasonable precautions, including password protection and document protection, to prevent unauthorized use of their accounts. They should not share their passwords with another person and should change their passwords regularly. The account holder is responsible for any transaction performed using the password of a user account, even if the party performing the transaction is not the account holder himself.
* The School's computer systems should only be used for School-related matters as permitted. As with all School equipment, computer systems, including the school network, for personal or commercial purposes are strictly prohiICTed. The School's computer systems may not be used for any unlawful purpose, including, but not limited to, the collection, download, distribution of fraudulently or illegally obtained media documents and software. Use of external networks or services – including cloud services – must comply with acceptable use policies issued by the organizations providing those networks and services.
* Users cannot access any information, School software or other documents (including programs, subroutine library members, data and e-mail) without prior permission from the School's relevant personnel, information security officer or the relevant party; cannot modify, copy, move or remove such information, software and documents. Users may not copy, distribute, display or disclose third party software without prior permission from the licensor. Users may not install software that is not properly licensed for use on systems.
* No computer system belonging to the School may be used irresponsibly or in a way that interferes with the work of others. This; transmitting or making available content that is defamatory, offensive or harassing, as well as chain letters, unauthorized mass mailings, or unsolicited advertisements; deliberate, reckless or negligent damage to a system, material or information that does not belong to the user; deliberately interrupting electronic communications or otherwise violating the privacy of others or accessing information that does not belong to or is not for the user; including deliberate misuse or misuse of system resources; or downloading software or data into administrative systems from untrusted sources, such as freeware.
* The school is in no way responsible for the content that it does not provide to the computer systems itself. Users access content provided by others, accepting that they may consider it offensive, inappropriate or objectionable, and at the user's own risk. Computer systems are provided "AS IS" and "AS AVAILABLE". The School disclaims any liability for the accuracy, completeness and reliability of third-party content. The user is responsible for the information he/she holds or stores on his/her computer systems.
* The user (i) attempts any action to prevent the operation of computer systems or the use of said computer systems by others; (ii) uploading content that will overload computer systems; (iii) actions that will endanger the general security of computer systems and/or harm other users; (iv) the use or attempt to use software that interferes with or interferes with the operation of computer systems is strictly prohiICTed.
* In case of detection of any information regarding the violation of this policy by another person, or an error or "by-pass" of the security of computer systems, the incident must be reported to Sevgi Kindergarten E-Security Coordinator.
* Unauthorized or inappropriate use of school computer systems, including non-compliance with this policy, constitutes a violation of School policy and requires Disciplinary Board follow-up with Administration approval. Any questions regarding the application of this policy to a certain situation are forwarded to the Sevgi Kindergarten e-Safety Coordinator.

**REVIEW**

The responsibility for reviewing and updating this document belongs to the Sevgi Kindergarten e-Safety Commission. Changes and updates are published with the approval of the Administration. The review is done three times a year, at the beginning, middle and end of each semester.

**Members of the eSafety Group**

Recep GÜZELEL Fatma GÜRSOY Elif KONAKLI

 ASSISTANT DIRECTOR Preschool Teacher Preschool Teacher

 ESafety Coordinator

EMİNE ÖZDEMİR

Head Teacher

Software Specialist