**e-SECURITY AGREEMENT OF OUR PROJECT**

Our project team believes that virtual security (e-Security) is an indispensable element for the protection of children and adults in the digital world while using technology such as computers, tablets and mobile phones.

Our project team works to raise educational standards, encourage success, support the professional work of the staff and improve management functions.

Our project team aims to protect all our children and staff from potential damages in virtual environments and to ensure that the internet is used in the most effective way for educational purposes.

**Responsibilities of Teachers and Students within the Scope of E-Security are as follows:**

• Contributing to the development of online security policies.

• Reading and adhering 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 know how they may relate to children in their care.

Modeling good practices when using new and emerging technologies

• Link curriculum to online safety education whenever possible.

• Identifying individuals who are concerned and taking appropriate action by following school protection policies and procedures.

• Mark appropriate support for online security matters, internally and externally.

• Maintaining a professional attitude level in personal and personal use of technology, both indoors and outdoors.

• Emphasize positive learning opportunities.

• Taking personal responsibility for professional development in this area.

The main responsibilities of children and young people are:

• Contributing to the development of online security policies.

• Reading and adhering to the School's Acceptable Use Policies (AUPs).

• Respect 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 security issues.

 **Safer Use of Online Communication and Technology 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 Personal information of staff or students will not be published.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 School Principal will take overall publication responsibility for published online content and ensure that the information is correct 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 posted 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 by appropriately encrypted with a 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 pictures and videos posted online are used in accordance with the school image use policy.

• The school will ensure that all images and videos are covered in accordance with data security, Acceptable Use Policies, Code of Conduct, social media, and other policies and procedures such as the use of personal devices and mobile phones.

• In accordance with the image policy, written consent of the parents will always be obtained before the pictures / videos of the students are published electronically. Students' faces and personal information will be kept confidential at every stage of the project.

 **Users**

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

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

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

• Video conferencing will take place through formal and approved communication channels, following a robust risk assessment.

• Only main administrators will be given access to video conference administration areas or remote control pages.

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

**Content**

• When recording a video conference lecture, written consent will be obtained from all sites and participants. At the start of the conference the reason for the recording must be stated and video conference recording must be available to all parties. Recorded materials will be stored securely

• If third-party materials are to be included, the school will check whether this recording is acceptable to avoid infringing on the third party's intellectual property rights.

• The school will establish a dialogue with other conference participants before joining a video conference. If the school is not, the school will check that it has received the material appropriate for the classroom.

• Proper and safe use of the internet and related devices in classrooms

• Internet use is an important feature of educational access, and all children will receive age- and ability-appropriate education as part of the integrated school curriculum to support and assist them in developing strategies to address their problems. For more information, please access specific curriculum policies.

• Internet access of the school 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 staff are aware that they will not rely on filtering alone to protect children, and training in surveillance, classroom management and safe and responsible use is essential.

• Content; It will suit the age 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 recommending use at home.

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

• The school will ensure that staff and students accept Internet-derived material compliant with copyright laws and sources of information.

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

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

• The school uses the internet to enable our students and staff to communicate and collaborate in a secure and confidential environment.

**Students' Use of Personal Devices and Cell Phones**

• Students will be trained in the safe and appropriate use of personal devices and mobile phones.

• It is strictly forbidden to use information tools in a way that adversely affects education and training by making speeches, receiving audio and video, sending messages and e-mails, sharing them with their friends without the knowledge and permission of the school administration and the teacher, and also to have a telephone during school hours.

• All use of children's mobile phones and personal devices will be in accordance with the acceptable usage policy.

• Cell phones or personal devices cannot be used by students in lectures or during official school hours unless they are part of an approved and directed curriculum-based activity with the consent of a faculty member.

• Children's use of mobile phones or personal devices in an 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 are advised not to communicate with their children by mobile phones during school hours and contact the school administration. In exceptional cases, exceptions may be allowed 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 limits and consequences will be recognized.

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

**Responding to Online Incidents and Protection Issues**

• All members of the school, sexting, online / cyberbullying, etc. You will be informed of the variety of online risks that can be encountered, including. This will be highlighted in staff training and educational approaches to students.

• All members of the school, filtering, sexting, cyberbullying, illegal content violation, etc. will be informed about 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) incident involving child protection concerns, which will be recorded later.

• Complaints about misuse of the Internet will be handled within the school's complaints procedures.

• Online / cyberbullying complaints will be handled within the scope of the school's anti-bullying policy and procedure

Any complaints about misuse of staff will be directed to the principal.

• The school complaints procedure will be communicated to students, parents and staff.

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

• All members of the school should be aware of the importance of confidentiality and the need to follow formal school procedures to raise concerns.

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

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

• The school notifies parents of any concerns as needed.

 **As the project team, we undertake to comply with the rules during and after the project in accordance with the above "e-Security Agreement".**