

FATIH ISLAM SECEN SCIENCE AND ART CENTRE

E-SECURITY POLICY GOALS AND POLICY SCOPE

- Fatih Islam Secen Science and Art Centre 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.
- Fatih Islam Secen Science and Art Centre believes that the internet and information communication technologies are an important part of daily life. Therefore, young people should be supported to learn how to manage risks and develop strategies to react to them.
- Fatih Islam Secen Science and Art Centre has the obligation to provide quality internet access in order to raise educational standards, encourage success, support the professional work of the staff and improve management functions.
- Fatih Islam Secen Science and Art Centre is responsible for ensuring that all young people and staff are protected from potential harm online.
- This policy has been prepared for administrators, teachers, support staff, young people and parents.
- This policy applies to internet access and use of communication devices, including personal devices. It also includes school-supplied devices for remote use, such as laptops, tablets or mobile devices where young people, staff or other people work.

The responsibilities of all employees are as follows:

- Contributing to the development of online security policies.
- Reading and adhering to the Acceptable Use Policies.
- Being responsible for the security of school systems and data.
- To be aware of online safety and know how they can relate to young people in their care.
- Model good practice when using new and emerging technologies.
- Link the curriculum with online safety education as far as possible.
- To identify individuals who are concerned and take action by following school protection policies and procedures.

- Emphasize positive learning opportunities.
- Taking personal responsibility for professional development in this area.

The main responsibilities of young people are:

- Contributing to the development of online security policies.
- Reading and adhering to the School's Acceptable Use Policies.
- 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.
- Taking responsibility for protecting themselves and others online.
- Being responsible for their own awareness and learning of the opportunities and risks posed by new and emerging technologies.

Parents' main responsibilities are:

- 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.
- Identifying changes in behavior that indicate that the child is at risk of harm online.
- Seek help or support from school or other appropriate institutions if they or their children encounter problems or issues online.
- Contributing to the establishment of the school's online security policies.
- Using school systems, such as learning platforms and other network resources, in a safe and appropriate way.
- Being responsible for their own awareness and learning of the opportunities and risks posed by new and emerging technologies.

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 properly protected by encryption 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 images and videos posted online are used in accordance with the school's official usage policy.
- The school will ensure that all images and videos are covered in compliance 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 photos / videos of the students are published electronically.

Official video conference and webcam use for educational purposes

- The school recognizes that video conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential for the whole activity.
- All video conferencing equipment will be turned off when not in use and when available and will not be set to auto answer.
- External IP addresses will not be submitted to other sites.
- Video conference contact details will not be shared publicly.
- Video conferencing equipment will be kept securely and locked out when not in use if required.

- School video conferencing equipment will not be removed from school buildings without permission.
- Personnel will make sure that external video conferencing opportunities and / or tools are appropriately evaluated and ensure that the accounts and systems used to access incidents are appropriately secure and confidential.

Users

- Students will seek 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 students 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 granted access to video conference administration areas or remote- control pages.
- Private login and password information for educational video conferencing services will be provided 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 beginning 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

- Internet use is an important feature of educational access and all students will receive age- and ability-appropriate education to support and assist them in developing strategies to answer their problems as part of the integrated school curriculum. 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. It will be suitable for the age and abilities of the students.
- All school devices will be used in accordance with the School's Acceptable Use Policy and with appropriate safety precautions.
- Students will be trained in the effective use of internet research, 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.

Use of Personal Devices and Cell Phones

- The use of mobile phones and other personal devices by young people and adults will be decided by the school and covered in appropriate policies, including the School's Acceptable Use or Cell Phone Policy.
- Fatih Islam Secen Science and Art Centre is aware that personal communication with mobile technologies is an accepted part of daily life for young people, staff and parents; however, it requires such technologies to be used safely and appropriately in school.
- Use of personal devices and mobile phones will be enforced in accordance with the law and other appropriate school policies.
- The responsibility of any electronic device brought to the field belongs to the user. The school takes no responsibility for any loss, theft, or damage to such items. The

school accepts no responsibility for the potential or actual adverse health effects caused by such devices.

- Abuse or sending of inappropriate messages or content via mobile phones or personal devices is prohibited by any member of the community and any violation will be handled as part of the policy of discipline / behavior.



- All members of Fatih Islam Secen Science and Art Centre community are recommended to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of Fatih Islam Secen Science and Art Centre community are recommended 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 secret. Cell phones and personal devices should not be shared.
- All members of Fatih Islam Secen Science and Art Centre community are advised to make sure that their mobile phones and personal devices do not contain any content that is offensive, disparaging or otherwise contrary to school policies.

Students' 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 students' mobile phones and personal devices will be carried out 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.
- Students' use of their mobile phones or personal devices in the educational activity 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.
- It is recommended that parents do not 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 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.

Use of personal devices and mobile phones by staff

- Staff are not allowed to connect their personal phones or devices with children, young people and their families in a professional capacity, inside or outside the setting. Pre-existing relationships that will jeopardize this issue will be discussed with managers.
- Staff are not allowed to use personal devices such as cell phones, tablets or cameras to take photos or videos of students and only use equipment provided for this purpose.
- Staff do not use any personal devices directly with students and only use equipment provided by the school during lessons / 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.

- Personal mobile phones and devices of the staff are turned off / silent during class hours.
- Bluetooth or other forms of communication should be "hidden" or turned off during class hours.
- Personal cell phones or devices cannot be used during the academic year, unless permitted by the school administration in emergencies.
- Disciplinary action is taken in cases where a staff member violates school policy.
- The police will be contacted if a staff member has illegal content saved or stored on a mobile phone or personal device or has committed a criminal offense.
- Any claim involving personal use of mobile phones or devices by staff will be responded to by following school management policy.

Student Training

- An online security (eSafety) curriculum is created to raise awareness among students about the importance of safe and responsible internet use and takes place throughout the school.
- Training on safe and responsible use will be done before internet access.
- Student contributions will be sought in writing and developing school online safety policies and practices, including curriculum development and implementation.
- Students will be encouraged to read and understand the Acceptable Use Policy, appropriate for their age and abilities.
- All users will be informed that network and internet usage will be monitored.
- Acceptable Use prospects 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.
- Outside support will be used to complement and support schools' internal approaches to online security (eSafety) education.
- The school will reward students for using technology positively.
- The school will implement peer education to improve online safety in accordance with students' needs.

Staff Training

- Online safety (eSafety) policy will be formally provided and discussed for the participation of all employees and strengthened and emphasized as part of our responsibility to protect.
- Staff will be aware that Internet traffic can be monitored and tracked to a single user. Discretion and professional behavior are required when using school systems and devices.
- All members of staff, professionally and personally, will be provided with up-to-date and appropriate staff training on safe and responsible Internet use in a variety of ways on a regular (at least annual) basis.
- The school highlights useful online tools that staff should use according to the age and abilities of the students.

Parents Training

- Fatih Islam Secen Science and Art Centre acknowledges 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 statements school, online safety (eSafety) policy on school website and expectations.
- Parents will be encouraged to read the School's Acceptable Use Policy and discuss its impact with their children.
- Parents will be provided with information and guidance on online safety.
- Parents will be encouraged to role model positive behaviors for their children online.

Responding to Online Incidents and Protection issues

- All members of the school will be informed of the variety of online risks that can be encountered, including sexting, online / cyberbullying, etc. This will be highlighted in staff training and educational approaches to students.
- All members of the school will be informed about the procedure for reporting online security (eSecurity) concerns such as, filtering, sexting, cyberbullying, illegal content violation, etc.

- 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 complaint procedure will be communicated to students, parents and 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.
- The school notifies parents of any concerns as needed.
- Once any investigation is complete, the school will receive information, identify lessons learned, and implement changes as necessary.
- Parents and students need to work together with the school to solve problems.