eSafety Label - Assessment Form

Assessment form submitted by Erkan Erden for Simav Akdağ İlkokulu Müdürlüğü - 16.01.2023 @ 21:02:48

Infrastructure

Technical security

Question: Are all of your school computers virus-protected?

- **Answer:** Yes, all school computers are virus-protected.

We are MEB certified and do not access any inappropriate or violent content on our computers and smart boards. Also our google filters are turned on. In addition to the computers in our school, USB disk security programs are installed on the personal usb sticks of our teachers, and we take precautions against any virus infiltration that may come from outside or outside when they are used on computers and personal computers in common use. home computers and our teachers are aware of this.

Question: Is the school system protected by a firewall?

- **Answer:** Yes.

All of our computers have the certificate at the address http://sertifika.meb.gov.tr/ installed. Sites not allowed by this certificate are not allowed. In order to enter the sites allowed by the certificate, we formally inform the relevant unit of the ministry that our institution is affiliated with and get approval. If approved, we can enter the sites. We also have various virus protection software on our school computers. Windows firewalls are always on on teachers' computers and classroom smartboards.

Question: Are filtering levels uniform across schools or do they depend on user profiles (teacher, pupil, admin staff, etc.) and their level of maturity/seniority?

- **Answer:** There is a basic level of filtering which blocks pornography, violent and illegal content.

You can use the address http://sertifika.meb.gov.tr/. Publisher: T.R. Ministry of Education General Directorate of Innovation and Educational Technologies (YEĞİTEK) Against Konya Highway Teknikokullar 06500 Veterans Hospital, Ankara, Turkey Material information: ISBN: 978-975-11-5096-7 Name of Work: Result of Information Production Education and Educational Technologies Coordinators Workshop Notice Release Date: August 2019, Ankara

Pupil and staff access to technology

Question: Are staff and pupils allowed to use their own equipment on the school WiFi network? How is this monitored?

- **Answer:** Staff and pupils are able to access the WiFi using their own personal devices. Use is governed by a robust Acceptable Use Policy, which is agreed and understood by all.

Although the wifi cannot be fully monitored in our institution, the wifi passwords are updated periodically and given to the relevant parties when a name or a different activity is seen by viewing the people on the network. In addition, media literacy is provided under control by providing content to our students through google class applications, class dojo and eba. Within our school, primary school 1-4. As there are classrooms and pre-school classes, they usually bring their personal technological tools to school with their teacher's permission, and the usernames are within the teacher's knowledge. Students cannot come to school with their tablets or parents' phones and access the wifi network without the permission of the teacher. The password is updated regularly.

Data protection

Question: Do you consistently inform all school members about of the importance of protecting devices, especially portable ones?

- **Answer:** We asume all teachers know how to protect portable devices.

We talked about this in the answer to question 1 on this topic. Teachers know that when they use USB sticks on shared computers, USB sticks must be protected and virus-free. Otherwise, it cannot use USB memory on shared computers. It uses its shares as scanned by moving them with cloud programs or protected mails.

Question: How is pupil data protected when it is taken 'off site' or being sent by email?

- **Answer:** All sensitive pupil data is encrypted and stored separately from the learning environment that pupils use.

1- Information was given to teachers, parents and students within the scope of the Law on Protection of Personal Data No. 6698. 2- It is clearly stated in the 11th article and other articles of the Ministry of National Education's Social Activity Permit Directive, and our school acts in accordance with this directive and the law. 3- Student information and data are included in the e-school area within the secure MEBBIS system of our Ministry. In addition, if parents want student information, they can get some necessary information from the e_state system, which is the secure platform of our state. By e-mail, we only send the information to the destination. We do not send information.

Software licensing

Question: Does someone have overall responsibility for licensing agreements?

- **Answer:** Yes.

Our school principal is primarily responsible for the school. In addition, our parent-teacher association and school purchasing commissions are responsible for purchasing licensed software. The Information Technologies Guidance teacher, who is interested in the education field of our school, is responsible for the installation of licensed software, monitoring and updating the license period. The most general auditor and the institution we are responsible for are the senior officials within the Ministry of National Education and the Ministry of Information Technologies.

Question: Has the school set a realistic budget for the software needs?

› **Answer:** Yes.

An exact budget cannot be determined. Because the prices of the software change according to inflation and the dollar exchange rate. However, while the estimated budget is being prepared on the TEFBIS system, an estimated budget is allocated according to the current conditions in the name of informatics and software expenses among the expense items. This budget is provided to our schools within the scope of the 10 thousand school in Basic Education project determined by our Ministry in response to our request from the Ministry of National Education, Department of Basic Education. Our school is on the list of 10 thousand schools across the country. In addition, Akdağ Primary School Family Association and Simav District Directorate of National Education Support Services Unit contribute.

Question: Do you have an agreed process for installing software on the school system?

› **Answer:** Yes. We have an agreed, effective process.

Teachers can install the web 2.0 software they need on their classroom computers. However, system-modifying malware like "vpn-proxy" is blocked. There is no need for this in our education system. The system is already returning to the security warning. In addition, computers belonging to school fixtures are periodically scanned and examined by the IT consultant, and spyware or proxy routers are deleted. Teachers know that the computer and smart board in the classroom belong to the school administration and do not install unnecessary and harmful software for personal use. Teachers can only download educational content, documents, videos, etc. from secure sites. can download. can download. can download, install. Ethical contracts are signed with teachers for this content upload and other behaviors.

IT Management

Question: Are teachers and pupils allowed to install software to computers that are school property?

› **Answer:** Yes.

As we mentioned in question 7, teachers can only download educational content from trusted sites and sources to school and classroom computers. Non-educational applications, personal-purpose programs cannot be installed from unsafe sources. However, our students cannot upload. The teacher uploads the necessary programs according to the curriculum and achievements. Our school already consists of kindergarten and primary school (4,5-9 years old) students. Students cannot upload anything without the knowledge of the teacher and administration. Students (MEB Certificate) can download pictures from sites permitted by the certificate while doing their homework. These are regularly deleted in a controlled manner.

Policy

Acceptable Use Policy (AUP)

Question: Does the school have a policy on the use of mobile devices / mobile phones?

› **Answer:** Yes.

Certified school Wi-Fi network, not private internet, is allowed to use mobile devices such as cell phones and tablets inside the school. Teachers cannot use their mobile devices privately during class hours.

Reporting and Incident-Handling

Question: Is there a procedure for dealing with material that could potentially be illegal?

- **Answer:** Yes.

https://basinmus.meb.gov.tr/meb_iys_dosyalar/2021_04/12123508_Sosyal_Medya_KYlavuzu.pdf http://simavakdagilkokulu.meb.k12.tr/ https://orgm.meb.gov.tr/www/brosurler/icerik/1364 https://orgm.meb.gov.tr/meb_iys_dosyalar/2019_12/26113028_GUVENLY_YNTERNET_KULLANIMI.pdf

Question: Does your school have a strategy in place on how to deal with bullying, on- and offline?

- **Answer:** Yes, we have a whole-school approach, addressing teachers, pupils and parents. It is also embedded into the curriculum for all ages.

According to the instructions in the 5th question answer, we have our own arrangements and transfer programs.

Question: Is there a clear procedure if pupils knowingly access illegal or offensive material at school?

- **Answer:** Yes. This is included in written guidance for staff.

Students and teachers cannot knowingly and voluntarily access information that contains unlawful insults within the school. Because our school uses the internet network of the Ministry of National Education and such situations are already banned as a banned site. A warning appears on the screen. cannot enter.

Staff policy

Question: Is there a School Policy that states how staff should behave online?

- **Answer:** Yes, we have regularly updated guidelines clearly laid out in the School Policy on this.

Decisions on the subject were taken by the teachers' board and our teachers were informed about the subject.

Pupil practice/behaviour

Question: Is there a school wide hierarchy of positive and negative consequences to address pupils' online behaviour?

- **Answer:** Yes and this is clearly understood by all and applied consistently throughout the school.

In this context, we follow the comments graphically by organizing surveys for our parents and students via google foms.

Question: When discussing eSafety related aspects, do pupils have the possibility to shape (extra-curricular and curricular) school activities based on what is going on in their daily lifes?

- **Answer:** Pupils are actively encouraged to choose topics of their interest and/or shape extra-curricular activities.

School presence online

Question: Is it possible for pupils to take part in shaping the school online presence?

- **Answer:** Yes, pupils have the possibility to feedback on our online presence.

http://simavakdagilkokulu.meb.k12.tr/icerikler/guvenli-cocuk_10223409.html https://www.facebook.com/Akdagilkokulu simavakdagilkokulu.meb.k12.tr https://twitter.com/AkdagIlkokulum

Question: Does the school have an online presence on social media sites?

- **Answer:** Yes.

https://www.facebook.com/Akdagilkokulu https://twitter.com/akdagilkokulum http://simavakdagilkokulu.meb.k12.tr/

Question: Is someone responsible for checking the online reputation of the school regularly?

- **Answer:** Yes.

school principal, school web management team, classroom teachers

Practice

Management of eSafety

Question: Technology develops rapidly. What is done to ensure that the member of staff responsible for ICT is aware of new features and risks?

- **Answer:** The job description outlines that the member of staff responsible for ICT needs to keep up to date on technologies.

Our students are educated with simple content such as media literacy and dezerformation, communication and the internet of things, while our teachers are given certificates, recorded and trained in the form of distance education and face-to-face education. In addition, parent permission documents are obtained for the use of students' visuals in social networks projects and activities. A social media publication and usage ethics form has been communicated to all our personnel in return for their signature, and a sense of responsibility has been given.

Question: How involved are school governors/school board members in addressing eSafety issues?

- **Answer:** There is a named school governor/ board member who reviews eSafety matters.

This person is our school principal, Erkan ERDEN. In addition, web monitoring and follow-up board members are elected at our school members' general assembly meetings at the beginning of the

year. these members are a board consisting of two teachers who understand computers and technology under the chairmanship of a principal or vice principal.

eSafety in the curriculum

Question: Do you include sexting and the school’s approach to it in your child protection policy?

› **Answer:** Yes, sexting is referenced in the child protection policy and there are clear guidelines on how to deal with incidents.

Many regulations and directives binding our institution on the subject have been communicated to schools by our ministry. In addition, within the scope of our school's security policy, every year parents, students and stakeholders are informed by adhering to legal bases. It is published on our school website.

Question: Is the eSafety curriculum progressive?

› **Answer:** Yes.

Definitely progressive. Because every unconscious movement can put our little students and adults in a difficult situation. because there are many malicious people in this technology world. We should not leave too much of our digital footprints or leave them protected.

Question: Do you talk about online extremism/radicalisation/hate speech as part of your online safety curriculum?

› **Answer:** We will respond to any questions about this from pupils, but these issues are not routinely part of our online safety education.

Thinking that these issues will confuse primary school students, we teach good values with better concepts instead of bad ones. We teach the sacrifices, respect and tolerance that living together requires. We convey to students that hate will harm themselves first, with content such as cartoons, animated films, etc.

Extra curricular activities

Question: Does your school celebrate 'Safer Internet Day'?

› **Answer:** Yes, the whole school celebrates 'SID'.

Güvenli internet günü her yıl 11 Şubat'ta kutlanmaktadır. Özellikle eTwinning projelerimizin planlanmasında bugüne özel bir yer ayırıyoruz. eTwinning tasarımları dışında proje yapmayan arkadaşlar için de genel bilgilendirme seminerleri ve etkinlikleri düzenliyoruz.

Sources of support

Question: Do pupils have a means to address a trusted adult in confidence if an online incident occurs outside the school?

› **Answer:** Yes, the school counselor is knowledgeable in eSafety issues.

Boards have been arranged for e-security within the school, and the phone numbers of all school

personnel have been written in visible places. In order for our students and parents to reach these numbers and names, it is presented as a poster to the relevant places by stating where and what the responsible persons are related to.

Question: Are there means in place that allow pupils to recognise good practise and expert knowledge in peers with regards to eSafety issues?

- **Answer:** We actively encourage pupils to become peer eSafety mentors by offering facultative courses and/or school rewards on eSafety topics or similar.

We raise awareness of students and families by inviting counselors, informatics experts and religious (religious) officials to our school and have them give seminars on these issues.

Staff training

Question: Do all staff receive regular training on eSafety issues?

- **Answer:** Yes, all staff receive regular training on eSafety.

Question: Are teachers trained on the topic of cyberbullying?

- **Answer:** Yes, every teacher.