eSafety Label - Assessment Form

Assessment form submitted by MECİT GÜNDÜZ for Durugöl Ortaokulu - 03.02.2023 @ 14:17:51

Infrastructure

Technical security

Question: Is the school system protected by a firewall?

- **Answer:** Yes.

Within the scope of FATIH (Movement to Increase Opportunities and Improve Technology) Project, internet and IT tools' cards and secure usage execution is carried out. In this direction; establishment of traceable network management, centralized providing managed controlled Internet access, N controllers firewall and IT enabled applications are available.

Question: Are existing ICT services regularly reviewed, updated and removed if no longer in use?

- **Answer:** Yes, this is part of the job description of the ICT coordinator.

Duties of the teachers who will carry out the IT guidance of the Fatih Project: Operating system and various software used in IT supported classrooms established within the scope of Fatih Project To ensure that the course contents are kept up-to-date and in working order.

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.

The internet provider at the school, the ministry of national education (MEB), has blocked access to all kinds of harmful content. This access to sites is plugged into the MEB internet filtering network.

Pupil and staff access to technology

Question: Are staff and pupils allowed to use USB sticks on school computers?

- **Answer:** Yes, but how staff and pupils are allowed to use their USBs is clearly stipulated in our Acceptable Use Policy.

School staff and students should receive adequate training on how to use USB memory sticks in school information tools. To keep your staff and students safe while letting them do this, Acceptable We've also included the ground rules in your Usage Policy.

Question: What is the pupil/computer access in your school?

- **Answer:** There are specific computer labs, which can be booked by the teacher and the teachers make good usage of this option.

Information communication, including Internet access and personal devices This security policy is valid for the use of your devices. children, staff or remote use to others, such as the laptops, tablets, or mobile devices they are working with This also applies to school-issued devices.

Data protection

Question: How are staff and pupil passwords generated for access to your school system?

- **Answer:** All users are attributed a different password by the system.

You can log in to the e-School parent information system as follows; First, log in to e-Okul.meb.gov.tr. Then you will see; A screen will appear listed as 'Student ID Number', 'Student School Number' and 'Numbers in the Picture'. Then, after filling all these fields, click on the 'Login' option at the bottom. Those who forget their password to do these operations can get a new password by clicking the link below.

Question: How is the storage of school records and other documentation dealt with over time?

- **Answer:** We have a school retention plan specifying how long specific kinds of records are being kept and how they should be archived/disposed of.

REGULATION ON GOVERNMENT ARCHIVE SERVICES Unit and Institution Archives Article 5 - Taxpayers may use "Unit Archives" for longer They establish “Institution Archives” for archival material or archival material that they will keep for a while. In the archives of the archival material unit archives held by the taxpayers for a period of 1-5 years; archival material, It is kept in the archives of the institution for 10-14 years.

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

- **Answer:** Yes, we provide training/manuals around issues like these.

A briefing is a press conference where brief information is given to an authorized person or administration. In particular, briefing meetings are held by managers on the protection of portable devices.

Software licensing IT Management

Question: What happens if a teacher would like to acquire new hard/software for the school network?

- **Answer:** It is up to the head teacher and/or ICT responsible to acquire new hard/software.

The person in charge of the IT network is fully aware of the school's equipment. to ensure that they are informed and that this is the School Policy and Acceptable Use. It is clearly stated in the policy. The person in charge of the network needs to be mindful of licensing responsibilities. Only school administrators and / or IT person can get new software. eTwinning, which is carried out within the scope of the European SchoolNet, It includes teachers in Europe such as Scientix, Europeana, Safer Internet Day. The concept of e-Security is given great importance in extensive studies in the field.

Question: Once new software is installed, are teachers trained in its usage?

- **Answer:** Yes, when we roll-out new software, training and/or guidance is made available.

Informing all school personnel about software licenses provision is important. This will mean that your systems can be secured and staff can try out software applications to assist with teaching and learning.

Policy

Acceptable Use Policy (AUP)

Question: How do you ensure the school policies are up to date?

- **Answer:** When changes are put into place at school that impact the policy, they are updated immediately.

When a change is made regarding e-Safety at your school, the school policies It is good practice to revise when necessary. However, outside of school It should be noted that changes can also affect policies such as new laws or changing technologies. Therefore, please review your policies at least once a year. is being reviewed.

Question: How does the school ensure that School Policies are followed?

- **Answer:** We have regular meetings where policy topics are discussed and non-conformity with the school policies is dealt with.

We have an e-Safety Policy and its negative or inappropriate situations are revised periodically. Ministry of National Education support services general directorate numbered 2018/10. In line with the circular on "Taking Security Measures", as Durugöl Secondary School; security policy file has been prepared. Life safety at school, internet safety, personal security themes based on the school policy. School safety policy, as required by the 2015/2018 strategic plan and all necessary e-security measures are taken.

Reporting and Incident-Handling

Question: Does the school take any responsibility for any online incidents that happen outside the school?

- **Answer:** Yes, and all staff, pupils and parents understand this.

Students are provided with eSafety support outside of the curriculum when requested. For all students to deal with online security issues It is important that we offer support. Students are given training on how to use online technology outside of school.

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

- **Answer:** Yes.

All personnel are required to deal with potentially illegal materials. should know the procedure. In such a case, the school superior who can take general responsibility A name should be chosen from the level leadership team. The procedure covers all of the School Policy. staff and students in the Acceptable Use Policy. must be clearly communicated. for Turkey Reporting can be made

on the web page.haberweb.org.tr.

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.

Some of the teachers of our school are cyberbullying, ICT, given by the Ministry of National Education. He received distance and face-to-face training on the correct and safe use of Our school has a strategy for how to deal with online and offline bullying. It is explained that the learning objectives of the eSafety champions online course (MOOC) are primarily to create your personalized eSafety strategy. Then consider the importance of appropriate eSafety policies in the context of the school; eSafety risks and challenges your school and students may face determining; teachers, parents, school management team, ICT experts, etc. Developing an eSafety strategy suitable for your school's needs with the participation of importance is emphasized.

Question: Is there a clear procedure detailing what to do if inappropriate or illegal material is discovered?

- **Answer:** Yes.

All personnel are required to deal with potentially illegal materials. should know the procedure. In such a case, the school superior who can take general responsibility A name should be chosen from the level leadership team. The procedure covers all of the School Policy. staff and students in the Acceptable Use Policy. must be clearly communicated. for Turkey Reporting can be made on the web page.haberweb.org.tr.

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.

It is ensured that all personnel, including new personnel, are aware of the policy regarding online behavior. This has been an issue that is regularly discussed at staff meetings and is expressly accepted in the School Policy and open to staff and students in the (AUP) Acceptable Use Policy.

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.

Evaluation of student opinions is made about the members of the organization that evaluates the student opinions of the school. Evaluation of Student Behaviors Rewarding students according to expected behaviors and as a result of the negative behaviors of the students and the sanctions to be applied. Behaviors that require sanctions are given warning, reprimand and school change or more severe punishments. For example; Behaviors that require reprimand: It is to record or broadcast an audio or video without permission in a way that violates personal rights through information tools or social media.

School presence online

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

- **Answer:** Yes.

Duties of the teachers who will carry out the IT guidance of the Fatih Project: Responsible for the web publishing team for the preparation, publication and updating of the school website. is to do.

Question: Does your school policy contain a section on the taking and publishing of photographs of, and by, pupils, parents and staff?

- **Answer:** Yes, we have a comprehensive section on this in our School Policy.

inistry of National Education General Directorate of Legal Services dated 07.03.2017 and numbered 2975829 In accordance with the article on the Use of Social Media in Schools numbered 2017-12, students, for security reasons, taking and posting photos of parents, staff prohibited. Mobile by visitors and parents to take photos or videos Use of phones or personal devices must be done in accordance with the school picture use policy.

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 member of staff responsible for ICT is sent to trainings/conferences at regular intervals.

Our IT formatter responsible for Information and Communication Technologies and has this title, but is sent to trainings / conferences voluntarily and at regular intervals, although her duty is different.

Question: Is there one single person responsible for ICT usage and online access in your school?

- **Answer:** Yes.

The person in charge of the IT network is fully aware of the school's equipment. to ensure that they are informed and that this is the School Policy and Acceptable Use. It should be clearly stated in the policy. The person in charge of the network needs to be mindful of licensing responsibilities. Only school administrators and / or IT person can get new software.

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.

In school SWOT analyzes, strategic plans, teachers' board meetings Current policies regarding e-Security are processed and put on the agenda. School teachers and students should be sensitive and conscious about e-Security, It is important that they keep their information up-to-date under

the guidance of the school administration. At staff meetings It is an issue that is regularly discussed and explicitly accepted in the School Policy and open to staff and students in the Acceptable Use Policy.

Question: Does the school have a designated member of staff responsible for eSafety?

- **Answer:** It is a shared responsibility for all staff.

All personnel are required to deal with potentially illegal materials. should know the procedure. In such a case, the school superior who can take general responsibility A name should be chosen from the level leadership team. The procedure covers all of the School Policy. staff and students in the Acceptable Use Policy. must be clearly communicated. for Turkey Reporting can be made on the web page.haberweb.org.tr.

eSafety in the curriculum

Question: Is (cyber)bullying discussed with pupils as part of the curriculum?

- **Answer:** Yes, we make this a priority in our school from a young age.

Trainings were given to all our classes from the police directorate of combating cybercrime in our school. Cyberbullying is a situation that can cause mental, psychological and emotional problems no matter what age group it is observed. Examples of bullying, especially among young people, darken the lives of many young people. In this case, both parents and teenagers need to be careful. Cyberbullying is a serious problem that cannot be ignored, and it also constitutes a crime in some cases.

Extra curricular activities

Question: Do pupils do peer mentoring about eSafety?

- **Answer:** Yes, on a regular basis.

e-Security continuous process, schools exchange information with peers and experts. educators provide examples from their personal experiences. It is emphasized that the participation phase is important. If all of these With eSafety tag communication tools (Blogs, Forums, Polls, Ambassadors Section) It is explained to our students on the page provided.

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.

Our vice principals, who are trained in e-security, can consult with all our teachers and staff, especially our IT formatter, English teachers and the e-security team formed by the school administration.

Question: Does the school provide eSafety support for parents?

- **Answer:** Yes, regularly.

We provide e-safety support to our parents. There is a FAMILY CHILD INTERNET USE AGREEMENT. They sign the Parent's Commitment and deliver it to our school.

Staff training

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

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

Integrated and online student and parent lessons on e-safety issues at our school security training is provided. All staff at our school receive training on internet security.

Question: Are teachers aware about the technology that pupils spend their freetime with?

- **Answer:** Yes, this is part of the training and/or information package provided to teachers.

Yes, especially our guidance counselor monitors students' online habits and informs.