eSafety Label - Assessment Form

Assessment form submitted by Denız Turan BIYIKLI for Mehmet Akif Ersoy Ortaokulu - 29.01.2021 @ 13:33:06

Infrastructure

Technical security

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

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

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:** Differentiated levels are applied to different ages of pupils and staff.Staff are able to request that certain sites are unblocked or blocked as appropriate.

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:** No, staff and pupils are not allowed to bring their own personal devices to school.

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.

Data protection

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

- **Answer:** Our email system is protected with passwords and firewalls, and we have rules in place about the transfer of pupil data.

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

- **Answer:** We store all school records in a safe environment.

Software licensing

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

- **Answer:** Yes.

Question: Does someone have overall responsibility for licensing agreements?

- **Answer:** Yes.

The school asıstant Ali Alay and the information technologies teacher Yelda Bilen are responsıble persons

IT Management

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

- **Answer:** There is a procedure in place that allows any staff member to make a request which will lead to an informed decision within a reasonable amount of days on wether new hard/software should be acquired.

Our school's e-safety board has procedures for this.

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

- **Answer:** Yes.

Information technologies teacher and school e security board are allowed if the conditions are suitable

Policy

Acceptable Use Policy (AUP)

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

- **Answer:** Yes.

It isdetailed in the e security policy on our school’s webrite

Question: Are eSafety issues referred to in other school policies (e.g. behaviour, anti-bullying, child protection)?

- **Answer:** Yes, eSafety is an integral part of several school policies.

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.

Reporting and Incident-Handling

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

- **Answer:** Yes, but this responsibility has not been communicated to everyone.

After any inuestigation is completed the school will get information determine lesson learne and implement cahnges as necessory

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

- **Answer:** Yes.

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.

Staff policy

Question: Are teachers permitted to use personal mobile devices in the classroom?

- **Answer:** No.

• Teachers will ensure taht any use os personel phones and devices is always carried out in accordance with data protection and revlant school policy and procedures. • Teacher' s personel cell phones and devices are turned off during class hours and put into silent made. • Bluetooth or other forms of communication must be hidden orturned off during class hours • Disciplinary action is taken'in cases which a techer violates schol policy • If a teacher has illegal content stored a mobile phone or personel device or has committed offense it will be sent to the police • Teacher will respond to any cloim inuoling their personeluse of the mobile phone or device by follwing the schol administration 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.

Pupil practice/behaviour School presence online

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

- **Answer:** No.

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.

The peer group students formed by the e safety board of the school inform the e safety board of the school by taking the feelings , thoughts and suggertions of their peers about our schoo's online policy . It is includede in our online policy ıf the board approves

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.

eSafety in the curriculum

Question: Are legal consequences of online actions discussed with pupils? Topics would include terms and conditions, online payments, copyright.

- **Answer:** Yes, in all grades.

Our parents do not have enough information about online security due to the location of our school and the limited opportunities in the region. We, as an institution, inform both parents and students by organizing various trainings, seminars and distributing leaflets.

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.

Question: Are pupils taught about their responsibilities and consequences when using social media? Topics would include digital footprints and data privacy.

- **Answer:** Yes, from an early age on.

We have an informative article about digital footprints in the e security section of our school website.

Question: Are pupils taught about the risks of sexting?

- **Answer:** Yes, sexting is integrated into our eSafety and our sex education teaching at appropriate times.

Considering the increase in child sexual abuse in our country, we regularly provide training at all levels according to the levels.

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.

Extra curricular activities

Question: Does the school provide eSafety support for pupils outside curriculum time?

- **Answer:** Yes.

Question: Do pupils do peer mentoring about eSafety?

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

They regularly give training to the peer group formed by the e-security board of the school. The peer group provides peer counseling with these trainings.

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

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

Safe internet day is celebrated by distributing informative brochures to parents and by doing various activities with teachers, staff and students at our school.

Sources of support

Question: Are other school services involved in eSafety issues (e.g. counsellors, psychologists, school nurse)?

- **Answer:** Yes, we have some support from them.

Staff training