

Assessment form submitted by seda akpinar for Hürriyet Mesleki ve Teknik Anadolu Lisesi -
09.01.2023 @ 15:33:32

Infrastructure

Technical security

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 Ministry of National Education, the internet provider at the school, has blocked access to all kinds of harmful content. Access to these sites is blocked by the The Ministry of National Education internet filtering network. There is a projection and secure internet access network in every area where lectures are made in our school. Eba education and eTwinning portals are also used in lectures. The secure internet access network is used with a network security filter.

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.

This is done regularly as esafety is of much importance.

Pupil and staff access to technology

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.

Antivirus software was purchased to be used on the computers in our school and all computers and smartboards are virus protected.

Question: Are mobile phones and other digital devices allowed in school?

› **Answer:** Mobile phones are banned on the school site and/or in the classrooms.

we collect students' mobile phones before the lesson starts and at the end of the day we give back their phones. In certain circumstances only, in compliance with the AUP due to the potential learning benefits mobile phones and digital devices can be used in the classroom under teachers' authority.

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.

Users may not authorize anyone for any reason to use their School account. The account holder is responsible for any use of the school account. Users should take all reasonable precautions, including password protection and document protection, to prevent unauthorized use of their accounts. They should not share their passwords with another person and should change their passwords regularly. The account holder is responsible for any transaction performed using the password of a user account, even if the party performing the transaction is not the account holder himself.

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.

We give esafety information ans seminar in our school including all the staff. We do it both face to fasce and in online platforms.

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.

It is a shared task between the director, co-administrators and ICT coordinator. School's staff are aware of the procedure for new software and that all licenses are appropriate

Software licensing

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

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

Nobody can install except the ict coordinator. if the teachers want to install something they have to get in contact with him for the e-safety issues to be carried out effectively.

IT Management

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

- › **Answer:** No, this can only be done by the person in charge of the school ICT network.

Our school agreed on the Turkish ministry of education process for installing software.

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

- › **Answer:** Whenever staff members have a question about software they can contact the school helpdesk.

Policy

Acceptable Use Policy (AUP)



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

> **Answer:** Yes.

Question: Does your school have an Acceptable Use Policy (AUP)?

> **Answer:** Yes, there is an AUP which covers all members of the school community.

Our AUP covers all members of the school community and this can be seen from our AUP and board meeting agenda items

Reporting and Incident-Handling

Question: Are incidents of cyberbullying logged centrally?

> **Answer:** Yes, we log incidents and also record them via the eSafety Label incident handling form.

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

> **Answer:** Yes.

we have a written policy and defined rules are applied.

Staff policy

Question: Do you inform teachers about the risks that come with potentially non-secured devices, such as smartphones?

> **Answer:** Yes, they are clearly formulated in the School Policy and discussed in regular intervals.

Question: What happens to a teacher's account once s/he changes her/his role or leaves the school?

> **Answer:** The administrator is informed and immediately deactivates the teacher account or adjusts rights where possible.

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

> **Answer:** Yes.

Pupil practice/behaviour

Question: Does your school have a policy that states how pupils should communicate electronically at school?

> **Answer:** Yes, these are defined in the AUP and taught to pupils across the curriculum.

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.

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.



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.

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.

e-safety matters are reviewed regularly at school board meetings by school governor and board members and this can be seen from our school board meetings agenda items and our AUP

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

› **Answer:** Yes.

eSafety in the curriculum

Question: Are all pupils in your school taught about eSafety?

› **Answer:** Yes, all pupils in all year groups.

An online safety (e-Safety) curriculum is created and included throughout the school to raise awareness among students about the importance of safe and responsible internet use. Seminars on ICT addiction, correct and safe use of ICT, and Cyber Bullying are organized regularly by the guidance service. The school applies peer education to improve online safety in line with students' needs.

Extra curricular activities

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

› **Answer:** Yes.

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.

Question: Does the school provide eSafety support for parents?

› **Answer:** Yes, regularly.

Our school recognizes that parents have an important role to play so that children can become safe and responsible users of the internet and digital technology. Information and guidance for parents on online safety is available to parents in a variety of formats through meetings, brochures, messages.



Staff training

Question: Are teachers trained on the topic of cyberbullying?

› **Answer:** Yes, every teacher.

Seminars on ICT addiction, correct and safe use of ICT, and Cyber Bullying are organized regularly by the guidance service and Ministry of Education system ÖBA.

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

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

Up-to-date and appropriate staff training on safe and responsible Internet use, professionally and personally, is provided to all members of staff in various ways on a regular (at least annual) basis, through the ICT officer, the Ministry of Education's PPA, the in-service training platform.

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

› **Answer:** Informally, the school provides help on this.

