eSafety Label - Assessment Form

Assessment form submitted by Duygu Karagözlü for İnönü Anadolu Lisesi - 16.08.2023 @ 19:29:37

Infrastructure

Technical security

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.

In Turkey, Ministry of Education offers a filtered internet server to all schools. Certain applications are automatically bypassed by the server. Therefore, the protection is automatically done as we are a public school benefiting from the Ministry of Education's internet.

Pupil and staff access to technology

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

- **Answer:** Some teachers allow mobile phones to be used in class as part of the class activity, due to the potential learning benefits mobile phones and digital devices can bring to the classroom.

According to the disciplinary regulations of the Ministry of Education using mobile phones to take photos, record videos, or audios are banned in public schools. However, in many lessons like ICT or English for using some applications like Kahoot, and MentiMeter we allow students to use their phones during the activities. (Our students may bring mobile phones and portable devices to our school in accordance with the relevant regulations of the Ministry of National Education. Our students can use mobile devices and mobile phones under the supervision of a teacher in educational activities within the school.)

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.

We have virus programs at all school computers. So that we use these programs with security.

Data protection

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.

We have a school retention plan that specifies how long certain types of records should be kept and how they should be archived/destroyed, and is set out in our e-safety policy.

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.

Our students log in to our school system with the passwords they have created. Students are trained by informatics teachers and our school's e-safety team on creating secure passwords. Within the framework of our school's e-safety plan, students pay attention to the following rules when creating a secure password: All user and admin passwords must be at least eight (8) characters in length. Longer passwords and passphrases are strongly encouraged. Where possible, password dictionaries should be utilized to prevent the use of common and easily cracked passwords. Passwords must be completely unique, and not used for any other system, application, or personal account. Default installation passwords must be changed immediately after installation is complete. Every teacher's flash disc in the school is virus protected. They also use their flash disc as keys to open smart boards. Access to smart boards is provided by teachers only

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.

Our email system is protected by passwords and firewalls and we have rules in place regarding the transfer of student data. These issues are handled sensitively at our school.

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.

Our school believes that e-Safety is an essential element of safeguarding teenagers and adults in the digital world when using technology such as computers, tablets, mobile phones, or game consoles. Because of this reason, the face to face seminars have been organized for all school members.

Software licensing

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

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

Yes, We have an agreed, effective process. Our school's internet access and installation of programs are managed by experts.

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.

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.

training and guidance is provided when new software is introduced in our school.

Policy

Acceptable Use Policy (AUP)

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.

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

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

Yes, we have school policies including safeguarding and child protection, anti-bullying, behavior, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing/ICT

Reporting and Incident-Handling

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

- **Answer:** Yes.

We have a procedure for potentially illegal material and we cover it in our e-security policy.

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.

Teachers are informed about the risks posed by potentially unsafe devices such as smartphones

Question: What happens to a teacher's account onces 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.

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.

The key responsibilities of our school's Pupils are: • Contributing to the development of online safety policies. • Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them. • Respecting the feelings and rights of others both on and offline. • Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues. • At a level that is appropriate to their age, ability, and vulnerabilities: • Taking

responsibility for keeping themselves and others safe online. • Taking responsibility for their awareness and learning about the opportunities and risks posed by new and emerging technologies. • Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

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

- **Answer:** Yes.

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.

Our school policy includes a section on taking and posting photos of students, parents and staff

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

- **Answer:** Yes.

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.

Personnel responsible for Information and Communication Technologies are sent to trainings/conferences at regular intervals.

eSafety in the curriculum

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.

Yes, our students are taught their responsibilities and consequences when using social media. We are also working on the issue during the safe internet week.

Question: Are pupils taught about the risks of sexting?

- **Answer:** Sexting is not specifically mentioned but pupils are educated about the permanence of images and

risks associated with the use of social media and digital images.

Question: Is eSafety taught as part of the curriculum?

- **Answer:** Yes.

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.

All the teachers in our school inform our students about cyberbullying in their lessons. In addition, our school guidance service regularly organizes activities about cyberbullying for our students and parents regularly

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

- **Answer:** Yes, we have integrated discussion and education about these issues into our curriculum.

Online extremism/radicalization/hate speech is mentioned as part of your online safety curriculum, we have integrated discussion and training on these topics into our curriculum.

Extra curricular activities

Question: Does the school have any up-to-date information about the online habits of pupils?

- **Answer:** Yes, we have plenty of information.

The school has up-to-date information about students' online habits.

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.

Our counselor provides regular training to our students.

Staff training

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

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

Our teachers take online courses prepared by the ÖBA platform and the Ministry of National Education. In addition, our teachers also participate in seminars organized on international platforms