eSafety Label - Assessment Form

Assessment form submitted by AYŞE ÖZDEMİR for BALIKESİR ŞEHİT TURGUT SOLAK FEN LİSESİ - 28.12.2020 @ 13:45:32

Infrastructure

Technical security

Question: Is the school system protected by a firewall?

- **Answer:** Yes, but sometimes we have to bypass it for certain applications.

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.

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.

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 Ministry of Education using mobile phohes 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,MentiMeter we allow students to use their phones during the activities.

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

- **Answer:** Yes, there is no monitoring of this.

As our school uses Ministry of Education's safe internet server , it is automatically monitored.

Data protection

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.

For two years , in public schools it is obligatory to put instruction manuals next to every device and every user including the students and all the staff has to obey those rules.

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.

> **All pupil data is stored in e-school system of Ministry of Education. Only teachers and the menagement can reach this data by using their personal IDs and passcodes. In addition, all computers ın the mangement department and teachers' rooms are protected by passcodes.**

Question: Do you have separated learning and administration environments in your school?

- **Answer:** No, they are on the same server.

> **As our school moved to another building five years ago, we do not have different servers for different environments as it was in our previous building in which we used FATİH project server. However,our insfracture has been started to be built. When it completed like all the public schools in Turkey , we will start to use FATİH project server which will enable us sepearte the environments.**

Software licensing

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

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

Question: How is the software and license status managed?

- **Answer:** It is part of responsibility of the IT responsible to be able to produce an overview of software and license status at any moment.

Question: Does someone have overall responsibility for licensing agreements?

- **Answer:** Yes.

> **All the aggreemnets for licencing is done by the Ministry of Education for public schools and in our school the responsible preson to follow the process is our ICT teacher.**

IT Management

Policy

Acceptable Use Policy (AUP)

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

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

> **All devices have instructional manuals which are obligatory in public schools.**

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

- **Answer:** Teachers and pupils have to sign the policy. In the case of pupils it is read and discussed in class.

We do not sign the policy; however if you are a public school teacher, an officer working in a government school, and if you enroll a public schhol all the regulations and rules are assumed to be accepted by the individual. We have to obey all the policies agrred by the Ministry of Education.

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.

For public schools all of which are managed by the Ministry of Education, we have common regulations.

Reporting and Incident-Handling

Question: Are incidents of cyberbullying logged centrally?

› **Answer:** Not really, handling cyberbullying incidents is up to the individual teacher.

As the quilts and punishments are certain with the regulation of discipline in public schools ,as teachers if we face a cyberbullying , the process is followed according to the regulation.

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

› **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: 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.

As we have instructional manuals and dicipline regulation , every teacher has to obey the rules while using device.

Pupil practice/behaviour

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.

The students enrolling the school at the moment give feedback; however our gradutades set up their own web sites using school's name to shape the school's presence.

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

- **Answer:** Not officially, but the ICT coordinator/a senior teacher assumes this role.

Practice

Management of eSafety

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.

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.

From 18 /04/2016 to 29/04/2016 all teachers in our school participated in the course numbered 2016000098 4.01.01.02.028 - Fatih Projesi Etkileşimli Sınıf Yönetimi Kursu for being trained to use smart boards, devices safely. As Ministry of Education holds courses , we participate them online. They are on the system of EBA.

eSafety in the curriculum

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.

In 9th grade ICT lessons cirriculum, course 1 theme 1 includes all topics about sfae internet usage including sexting.

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.

Question: Is the eSafety curriculum progressive?

- **Answer:** Not really; we try to stay as close to the national curriculum as possible.

If we are able to get a label , we will follow the curriculum given by www.esafetylabel.eu.

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.

Extra curricular activities

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

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

Sources of support

Question: Does the school provide eSafety support for parents?

- **Answer:** Yes, when asked.

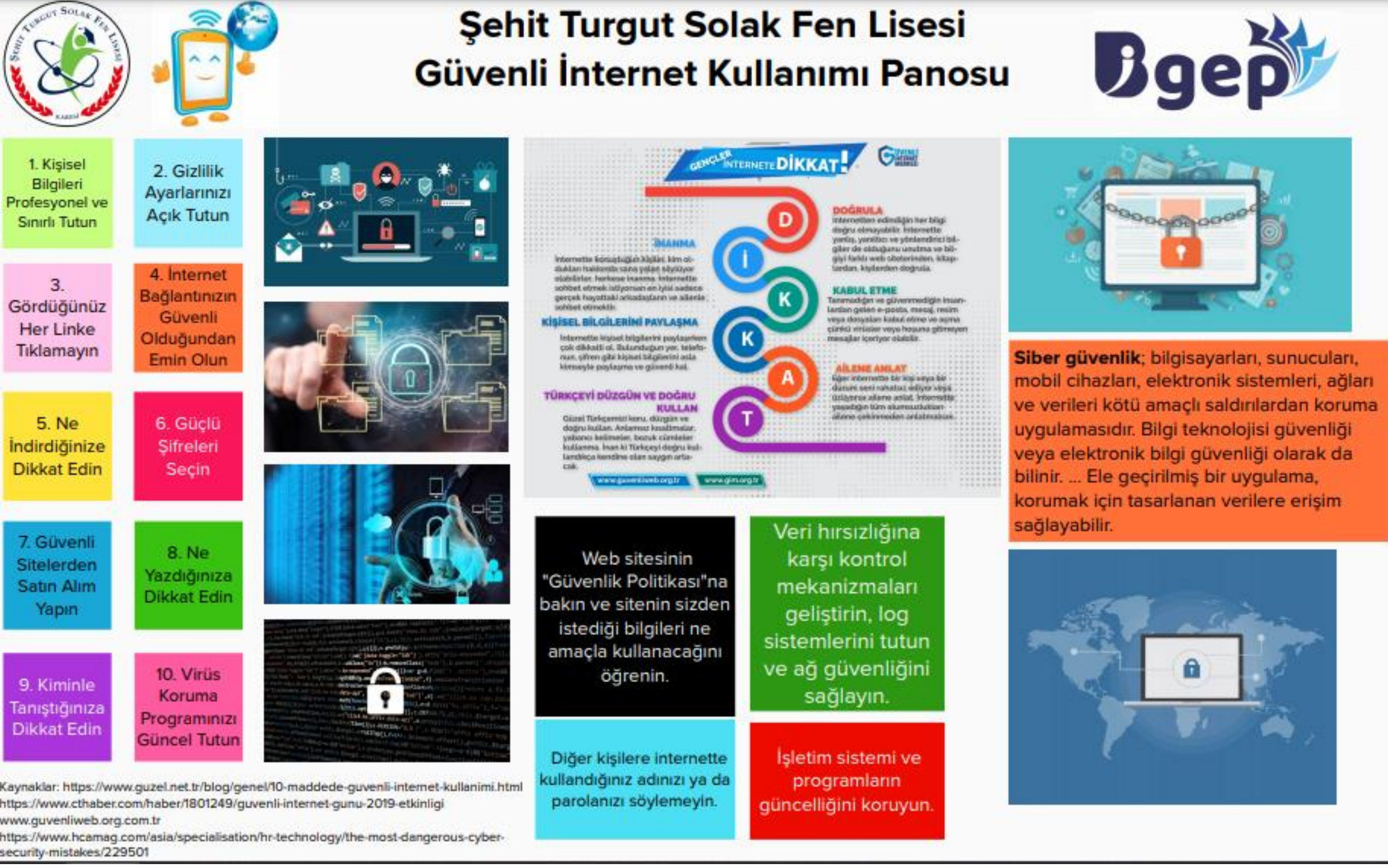
Staff training

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

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

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.



Şehit Turgut Solak Fen Lisesi Güvenli İnternet Kullanımı Panosu

1. Kişisel Bilgileri Profesyonel ve Sınırlı Tutun

2. Gizlilik Ayarlarınızı Açık Tutun

3. Gördüğünüz Her Linke Tıklamayın

4. İnternet Bağlantınızın Güvenli Olduğundan Emin Olun

5. Ne İndirdiğinize Dikkat Edin

6. Güçlü Şifreleri Seçin

7. Güvenli Sitelerden Satın Alım Yapın

8. Ne Yazdığınıza Dikkat Edin

9. Kiminle Tanıştığınıza Dikkat Edin

10. Virüs Koruma Programınızı Güncel Tutun

GENÇLER İNTERNETE DİKKAT!

D – DOĞRULA
İnternetten edindiğin her bilgi doğru olmayabilir. İnternette yanlış, yanıltıcı ve yönlendirici bilgiler de olduğunu unutma ve bilgiyi farklı web sitelerinden, kitaplardan, kişilerden doğrula.

İ – İNANMA
İnternette konuştuğun kişiler, kim oldukları hakkında sana yalan söylüyor olabilirler, herkese inanma. İnternette sohbet etmek istiyorsan en iyisi sadece gerçek hayattaki arkadaşların ve ailenle sohbet etmektir.

K – KABUL ETME
Tanımadığın ve güvenmediğin insanlardan gelen e-posta, mesaj, resim veya dosyaları kabul etme ve açma çünkü virüsler veya hoşuna gitmeyen mesajlar içeriyor olabilir.

K – KİŞİSEL BİLGİLERİNİ PAYLAŞMA
İnternette kişisel bilgilerini paylaşırken çok dikkatli ol. Bulunduğun yer, telefonun, şifren gibi kişisel bilgilerini asla kimseyle paylaşma ve güvende kal.

A – AİLENE ANLAT
Eğer internette bir kişi veya bir durum seni rahatsız ediyor veya üzüyorsa ailene anlat. İnternette yaşadığın tüm olumsuzlukları ailene çekinmeden anlatmalısın.

T – TÜRKÇEYİ DÜZGÜN VE DOĞRU KULLAN
Güzel Türkçemizi koru, düzgün ve doğru kullan. Anlamsız kısaltmalar, yabancı kelimeler, bozuk cümleler kullanma. İnan ki Türkçeyi doğru kullandıkça kendine olan saygın artacak.

www.guvenliweb.org.tr www.gim.org.tr

Web sitesinin "Güvenlik Politikası"na bakın ve sitenin sizden istediği bilgileri ne amaçla kullanacağını öğrenin.

Veri hırsızlığına karşı kontrol mekanizmaları geliştirin, log sistemlerini tutun ve ağ güvenliğini sağlayın.

Diğer kişilere internette kullandığınız adınızı ya da parolanızı söylemeyin.

İşletim sistemi ve programların güncelliğini koruyun.

Siber güvenlik; bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü amaçlı saldırılardan koruma uygulamasıdır. Bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinir. ... Ele geçirilmiş bir uygulama, korumak için tasarlanan verilere erişim sağlayabilir.

Kaynaklar: https://www.guzel.net.tr/blog/genel/10-maddede-guvenli-internet-kullanimi.html
https://www.cthaber.com/haber/1801249/guvenli-internet-gunu-2019-etkinligi
www.guvenliweb.org.com.tr
https://www.hcamag.com/asia/specialisation/hr-technology/the-most-dangerous-cyber-security-mistakes/229501

This school has been awarded with the eSafety Label

Bronze valid until 06/2022