eSafety Label - Action Plan

Action plan submitted by Murat ÇOLAK for MAÇKA CE-Zİ-NE KARDEŞLER İLKOKULU - 15.01.2021 @ 10:28:11

By submitting your completed Assessment Form to the eSafety Label portal you have taken an important step towards analysing the status of eSafety in your school. Congratulations! Please read through your Action Plan carefully to see what you can do to improve eSafety further in your school. The Action Plan offers useful advice and comments, broken down into 3 key areas: infrastructure, policy and practice.

Infrastructure

Technical security

- An educational approach and building resilience in pupils of all ages is also key to safe and responsible online use so bring together all teachers to have a discussion on how they will talk to their pupils about being a good and safe digital citizen. See www.europa.eu/youth/EU_en for examples of discussions that can take place in the classroom on this topic, through role-play and group games.

- It is good practice that your ICT services are regularly reviewed, updated and removed if no longer in use.

Pupil and staff access to technology

- There are clear advantages for staff and pupils to bring their personal devices to school and to access internet on them. Besides supplementing the technical equipment available at school, this provides an important link between learning at home and at school and an opportunity to guide young people in responsible use.
  However, staff and pupil use of their own equipment on the school network needs to be addressed in an Acceptable Use Policy so that users are clear about which networks they should use and why. The Acceptable Use Policy needs to include clear guidance about which activities are permitted while on the school network, and what is not allowed.

- The fact that staff and pupils are allowed to use USB memory sticks in your school following permission, would require that all staff concerned receive adequate training to be able to know when they can be used safely. Is this the case? To keep your systems secure whilst allowing staff and pupils you also need to include the ground rules in your Acceptable Use Policy. Check the fact sheet on Use of removable devices at www.esafetylabel.eu/group/community/use-of-removable-devices to make sure you cover all security aspects.

- Ensure that the policy on mobile phones is being applied consistently throughout the school. Take a look at the fact sheet on Using Mobile Phones at School (www.esafetylabel.eu/group/community/using-mobile-device-in- schools).

Data protection

- It is good that your email system is protected and that you have a policy for the transfer of pupil data in place. In

this regard, it is important to draw up guidelines so that all staff are clear about what to do if they discover inappropriate or illegal content on school machines. For further information see the fact sheet on Protecting sensitive data (www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools).

- Your new users are given a standard password and are asked to generate their own password on their first access. Passwords offer unique entry points into the school computing system and some basic rules of password security should be rigorously applied. For further information, read the fact sheet on Safe passwords at www.esafetylabel.eu/group/community/safe-passwords.
  Include these rules in your Acceptable User Agreement and avoid giving new users a standard “first access" password.

- It is good that your school provides training materials on the importance of protecting devices, especially portable ones. Please consider sharing those with others through the in . Also ensure that your materials are regularly reviewed to ensure they are in line with the state of the latest technology.

- There is a retention plan in place for your school detailing how specific school records are stored, archived and disposed. This is very good. Ensure that the plan is followed and review it regularly to ensure it relates to the Data Protection Act and other relevant legislation. Check the according fact sheet for more information.

Software licensing

- It is important to ensure that all new staff are briefed about the effective processes you have for the installation of new software. This will mean that the security of your systems can be maintained and that staff can try out new software applications that will help teaching and learning.

IT Management

Policy

Acceptable Use Policy (AUP)

- It is excellent that eSafety is an integral part of several school policies. Do all staff make reference to it when appropriate through their teaching? Look for examples of good practice and share these with staff and pupils. Produce a short case study to highlight this good practice and upload it to your profile on the eSafety Label portal via your My school area as inspiration for other schools.

- Regularly review the Mobile Phone Policy to ensure that it is fit for purpose and that it is being applied consistently across the school. The fact sheets on Using mobile phones at school (www.esafetylabel.eu/group/community/using-mobile-device-in-schools) and School Policy (www.esafetylabel.eu/group/community/school-policy) will provide helpful information.

- It is good that you have an Acceptable Use Policy for all members of the school community. Regularly review the AUP to ensure that it is still fit for purpose; to ensure that your AUP is sufficiently comprehensive, take a look at the fact sheet and check list on Acceptable Use Policy at www.esafetylabel.eu/group/community/acceptable- use-policy-aup-.

Reporting and Incident-Handling

- Have teachers received training on dealing with potentially illegal material? Is the procedure clearly indicated in the School Policy and the Acceptable Use Policy which all teachers and pupils have signed? All staff and pupils should be aware that they should report any suspected illegal content to the national INHOPE hotline (www.inhope.org).

Staff policy

- It is good practice that the school policy includes information about risks with potentially non-secured devices, such as smartphones and that reference is made to it. Consider sharing your school policy via the uploading evidence tool, also accessible through the My school area.

- As new technology and online practices emerge the borders of acceptable practice are constantly blurred. This is something that needs to be discussed at staff meetings often. Could you create a tutorial on professional online conduct of staff and upload it to your school profile via your My school area so that other schools can benefit from your good practice?

Pupil practice/behaviour

- Your school has a school wide approach of positive and negative consequences for pupil behaviour. This is good practice, please share your policy via the My school area of the eSafety portal so that other schools can learn from it.

School presence online

- We recommend that you specifically nominate a web-experienced staff member to periodically check the school's online reputation. Monitoring such an important aspect on an ad hoc basis only is insufficient. Remember that this is the image that prospective parents will receive when they search for your school online.

- Check the fact sheet on Taking and publishing photos and videos at school (www.esafetylabel.eu/group/community/taking-and-publishing-photos-and-videos-at-school) to see that your School Policy covers all areas, then upload this section of your School Policy to your profile page via your My school area so that other schools can learn from your good practice.

- Regularly check the content of the school's online presence on social media sites to ensure that there are no inappropriate comments. Set up a process for keeping the site/page up to date, and check the fact sheet on Schools on social networks (www.esafetylabel.eu/group/community/schools-on-social-networks) for further information to make sure that good practice guidelines have been followed. Get feedback from stakeholders about how useful the profile is.

Practice

Management of eSafety

- It is good that all staff in your school are responsible for eSafety. However, it is good practice to appoint a person who will have overall responsibility for eSafety issues to provide the focus needed. Ideally this should be

someone from the senior leadership team. Ensure that this person is involved in the development and regular review of your School Policy. She or he should not only be informed, but should also fill out the Incident handling form whenever an incident arises at www.esafetylabel.eu/group/teacher/incident-handling.

eSafety in the curriculum

- It is good that these issues have been included in the eSafety curriculum. It is a good idea to regularly review the issues which are being covered by your eSafety education in order to ensure that new and emerging issues are covered.

- It is good that eSafety is taught as part of the curriculum in your school. Ensure that all staff are delivering eSafety education where appropriate throughout the curriculum and not just through ICT or Personal Social and Health lessons. You/your staff may find some useful ideas and resources in the fact sheet Embedding eSafety in the curriculum at www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum.

- It is commendable that you are able to provide an eSafety curriculum that keeps up with emerging issues. Continue to make use of new resources as they are made available. Can you upload to your school profile an outline of how you design the curriculum and links to some of the resources you use – this would be most helpful for other schools.

- It is excellent that consequences of online actions are discussed with pupils in all grades. Terms and conditions need to be read to fully understand contractual conditions. This can also concern aspects of data privacy.
  Another important topic is breach of copyright. Please share the materials used through the uploading evidence tool, accessible also via the My school area.

Extra curricular activities

- It is good that you provide eSafety support for your pupils outside curriculum time when asked. Consider offering all pupils support to deal with online safety issues. It may be helpful to provide a “surgery" to help pupils to set their Facebook privacy etc. The eSafety Label portal provides resources that will be useful for this; check out the fact sheet on Pupils' use of online technology outside school at www.esafetylabel.eu/group/community/pupils- use-of-online-technology-outside-school.

Sources of support

- It is great that you have a staff member which is knowledgable in eSafety issues who acts as a teacher of confidence to pupils.

Staff training

- It should be a real benefit to your pupils that all staff receive regular training on eSafety issues. Continue to gather feedback from staff on the medium- and long-term benefits of the training and consult the eSafety Label portal to see suggestions for training courses at www.esafetylabel.eu/group/community/suggestions-for-online- training-courses.

- Your school makes sure that every teacher is trained on cyberbullying. Please share resources that are used in these trainings via uploading them to your My school area. Are you also monitoring the effect that this training

had on the number of incidents?

- It is good practise that you provide information to teachers on the technology used by pupils in their freetime. This is important as this awareness is the first step in addressing the issue of powering down for school. At the same time pupils should not be asked to do their homework using technology not available to them outside of schools. You might want to have a look at the Essie Survey of ICT in schools.

The Assessment Form you submitted is generated from a large pool of questions. It is also useful for us to know if you are improving eSafety in areas not mentioned in the questionnaire. You can upload evidence of such changes via the Upload evidence on the My school area section of the eSafety Portal. Remember, the completion of the Assessment Form is just one part of the Accreditation Process, because the upload of evidence, your exchanges with others via the Forum, and your reporting of incidents on the template provided are all also taken into account.

eSafety Label – Eylem Planı

Altyapı

Teknik Güvenlik

- Her yaştan öğrencide bir eğitim yaklaşımı ve dayanıklılık oluşturma, çevrimiçi güvenli ve sorumlu olmanın anahtarıdır. Öyleyse tüm öğretmenleri öğrencileriyle iyi ve güvenli dijital bir vatandaş olma konusunda nasıl konuşacaklarını tartışmak için bir araya getirin. Sınıflarda uygulanabilecek drama ve grup oyunları gibi tartışma örneklerini görmek için http://www.europa.eu/youth/EU_en
- Bilgisayar teknik servisinizin düzenli olarak gözden geçirilmesi, güncellenmesi ve artık kullanılmıyorsa değiştirilmesi iyi bir uygulamadır.

Öğrenci ve Personelin Teknoloji Erişimi

- Personel ve öğrencilerin kişisel cihazlarını okula getirmelerinin ve internete erişmelerinin açık avantajları vardır. Okulda mevcut olan teknik ekipmanı desteklemenin yanı sıra, bu evde ve okulda öğrenme ile gençlere sorumlu kullanım konusunda rehberlik etme fırsatı arasında önemli bir bağlantı sağlar. Ancak, personelin ve öğrencinin okul ağında kendi ekipmanlarını kullanması Kabul Edilebilir Kullanım Politikası'na hitap etmelidir. Bu, kullanıcıların hangi ağları neden kullanmaları gerektiği

konusunda net olmasını sağlar. Kabul Edilebilir Kullanım Politikası, okul ağındayken hangi faaliyetlere izin verildiği ve verilmediği konusunda net bir rehberlik içermelidir.

- Okulunuzda görevlilerin ve öğrencilerin izin aldıktan sonra USB bellek kullanmalarına izin verilmesi gerçeği, ilgili tüm personelin ne zaman güvenli bir şekilde kullanılabileceklerini bilmeleri için yeterli eğitim almalarını gerektirir. Durum bu mudur? Personel ve öğrencilere izin verirken sistemlerinizi güvende tutmak için Kabul Edilebilir Kullanım Politikanıza temel kuralları da dahil etmeniz gerekir. Taşınabilir araç kullanımı konusunda tüm güvenlik koşullarını sağlayıp sağlamadığınızı kontrol etmek için bilgi formunu kontrol edin. https://www.esafetylabel.eu/group/community/use-of-removable-devices
- Cep telefonlarına ilişkin politikanın okul genelinde tutarlı bir şekilde uygulanmasını sağlayın. Okulda cep telefonu kullanımı bilgi formuna göz atın. https://www.esafetylabel.eu/group/community/using-mobile-device-in-schools

Veri Koruma

- E-posta sisteminizin korunması ve öğrenci verilerinin yerinde aktarımı için bir politikanızın olması iyidir. Bu bağlamda, tüm personelin okul makinelerinde uygunsuz veya yasadışı içeriğin farkına vardıklarında ne yapacakları konusunda net olmaları için kılavuzlar hazırlamak önemlidir. Hassas veri koruma konusunda daha fazla bilgi için bilgi formu şu şekildedir: https://www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools
- Yeni kullanıcılarınıza standart bir şifre verilir ve ilk girişlerinde kendi şifrelerini oluşturmaları istenir. Şifreler, okul bilgi işlem sistemine benzersiz giriş noktaları ve bazı temel kurallar sunar. Şifre güvenliği titizlikle uygulanmalıdır. Daha detaylı bilgi için, Güvenli Şifreler bilgi formunu okuyun. https://www.esafetylabel.eu/group/community/safe-passwords
  Bu kuralları Kabul Edilebilir Kullanıcı Sözleşmenize dahil edin ve yeni kullanıcılara standart bir "ilk erişim" parolası vermekten kaçının.
- Okulunuzun, özellikle taşınabilir olan cihazların korunmasının önemi konusunda eğitim materyalleri sağlaması iyidir. Lütfen bunları girişte başkalarıyla paylaşmayı düşünün. Ayrıca malzemelerinizin en

son teknoloji ile uyumlu olduklarından emin olmak için düzenli olarak gözden geçirildiğinden emin olun.

- Okulunuz için, belirli okul kayıtlarının nasıl saklandığını, arşivlendiğini ve yok edildiğini gösteren bir saklama planı mevcuttur. Bu oldukça iyidir. Planın takip edildiğinden emin olun ve Veri Koruma Yasası ve diğer ilgili mevzuatla ilgili olduğundan emin olmak için düzenli olarak gözden geçirin. Daha fazla bilgi için ilgili bilgi formunu inceleyin.

Yazılım Lisanslama

- Yeni yazılım kurulumu için sahip olduğunuz etkili süreçler hakkında tüm yeni personelin bilgilendirildiğinden emin olmak önemlidir. Bu, sistemlerinizin güvenliğinin korunabileceği ve personelin öğretmeye ve öğrenmeye yardımcı olacak yeni yazılım uygulamalarını deneyebileceği anlamına gelir.

BT Yönetimi

İlke

Kabul Edilebilir Kullanım Politikası (AUP)

- E-Güvenlik'in çeşitli okul politikalarının ayrılmaz bir parçası olması mükemmeldir. Tüm personel öğretim süresince uygun olduğunda ne zaman başvuruda bulunur? İyi uygulama örneklerini araştırın ve bunları personel ve öğrencilerle paylaşın. Bu iyi uygulamayı vurgulamak için kısa bir vaka çalışması hazırlayın ve bunu diğer okullar için ilham kaynağı olarak http://www.esafetylabel.eu/group/teacher/my-school-area aracılığıyla e-Güvenlik Etiketi portalındaki profilinize yükleyin.
- Cep Telefonu Kullanımı Politikasını amaca uygun olduğundan ve uygulandığından emin olmak için okul genelinde düzenli olarak gözden geçirin. Okulda cep telefonu kullanımı konusunda gerekli bilgiyi edinebileceğiniz bilgi formu https://www.esafetylabel.eu/group/community/using-mobile-device-in-schools ve okul politikası konusunda yardımcı olacak bilgi formu https://www.esafetylabel.eu/group/community/school-policy şeklindedir.
- Okul topluluğunun tüm üyeleri için Kabul Edilebilir Kullanım Politikasına sahip olmanız çok iyi. Hala amaca uygun olduğundan emin olmak için ve Kabul Edilebilir Kullanım Politikanızın yeterince

kapsamlı olduğundan emin olmak için Kabul Edilebilir Kullanım Politikası hakkındaki bilgi formu ve kontrol listesini içeren şu adrese bir göz atın:

https://www.esafetylabel.eu/group/community/acceptable-use-policy-aup-

Raporlama ve Olay Yönetimi

- Öğretmenler potansiyel yasa dışı materyallerle başa çıkma konusunda eğitim aldı mı?

  Tüm öğretmenlerin ve öğrencilerin imzaladığı Okul Politikası ve Kabul Edilebilir Kullanım Politikası'nda prosedür açıkça belirtilmiş mi? Tüm personel ve öğrenciler yasadışı olduğundan şüphelenilen içeriği ulusal INHOPE yardım hattına bildirmeleri gerektiğinin farkında olmalıdırlar (http://www.inhope.org/).

Personel Politikası

- Okul politikasının, akıllı telefonlar ve buna benzer referanslar gibi potansiyel olarak güvenli olmayan cihazlarla ilgili riskler hakkında bilgi içermesi iyi bir uygulamadır. Okul politikanızı http://www.esafetylabel.eu/group/teacher/my-school-area kısmından da erişilebilen yükleme kanıt alanından yüklemeyi göz önüne alın.
- Yeni teknoloji ve çevrimiçi uygulamalar ortaya çıktıkça, kabul edilebilir uygulamaların sınırları sürekli olarak bulanıklaşmaktadır. Bu personel toplantılarında sık sık tartışılması gereken bir konudur. Diğer okulların iyi uygulamanızdan yararlanması için http://www.esafetylabel.eu/group/teacher/my-school-area aracılığıyla okul profilinize yükleyeceğiniz personelin profesyonel çevrimiçi davranışı konusunda bir eğitim oluşturabilir misiniz?

Öğrenci Uygulaması / Davranışı

- Okulunuzun, öğrenci davranışları için olumlu ve olumsuz sonuçlara dair okul çapında bir yaklaşımı vardır. Bu iyi bir uygulamadır ve lütfen politikanızı E-Güvenlik sitesinde http://www.esafetylabel.eu/group/teacher/my-school-area kısmından diğer okulların da bunu öğrenebilmeleri için paylaşın.

Çevrimiçi Okul Varlığı

- Okulun çevrimiçi itibarını periyodik olarak kontrol etmesi için web konusunda deneyimli bir personel atamanızı öneririz. Böylesine önemli bir konuyu yalnızca yüzeysel izlemek yetersizdir. Bunun, potansiyel ebeveynlerin okulunuzu çevrimiçi olarak arattıklarında görecekleri resim olduğunu unutmayın.
- Okul politikanızın Okulda Fotoğraf ve Video Çekip Yayınlama konusunda bütün gereklilikleri karşılayıp karşılamadığını görmek için https://www.esafetylabel.eu/group/community/taking-and-publishing-photos-and-videos-at-school bilgi formunu inceleyin ve daha sonra bu iyi uygulamadan diğer okulların yararlanabilmesi için okul politikanızın bu kısmını Okul Politikası profil sayfanıza http://www.esafetylabel.eu/group/teacher/my-school-area kısmından yükleyin.
- Uygunsuz yorumlar olmadığından emin olmak için okulun sosyal medya sitelerindeki çevrimiçi varlığının içeriğini düzenli olarak kontrol edin. Siteyi / sayfayı güncel tutmak için bir süreç oluşturun ve iyi uygulama yönergelerinin takip edildiğinden emin olmak için sosyal ağlardaki okullara yönelik bilgi formunu https://www.esafetylabel.eu/group/community/schools-on-social-networks bölümünden kontrol edin. Profilin ne kadar yararlı olduğu hakkında paydaşlardan geri bildirim alın.

Uygulama

E-Güvenlik Yönetimi

- Okulunuzdaki tüm personelin e-Güvenlik'ten sorumlu olması iyidir. Ancak, ihtiyaç duyulan odağı sağlamak için e-Güvenlik konularında genel sorumluluk sahibi olacak bir kişinin atanması iyi bir uygulamadır. İdeal olarak bu üst düzey liderlik ekibinden biri olmalıdır. Bu kişinin, Okul Politikanızın gelişimi ve gözden geçirilmesi sürecine dahil olduğundan emin olun. Herhangi bir durum oluştuğunda bu kişi yalnıza bilgilendirilmemeli; aynı zamanda http://www.esafetylabel.eu/group/teacher/incident-handling bölümünden vaka tutanağı doldurmalıdır.

Müfredatta E-Güvenlik

- Bu konuların e-Güvenlik müfredatına dahil edilmiş olması iyidir. e-Güvenlik eğitiminizin kapsamına giren konular, yeni ve ortaya çıkan sorunların dahil olduğundan emin olmak adına konuları düzenli olarak gözden geçirmek iyi bir fikirdir.
- E-Güvenlik'in okulunuzda müfredatın bir parçası olarak öğretilmesi iyidir. Sadece Bilişim Teknolojileri veya Kişisel, Sosyal ve Sağlık dersleriyle değil; müfredat süresince uygun olan yerlerde tüm personelin e-Güvenlik sağladığından emin olun. Siz / personeliniz, müfredata e-Güvenliği Belgeye Gömme bilgi sayfasında bazı yararlı fikirler ve kaynaklar bulabilirsiniz: https://www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum
- Ortaya çıkan sorunlara ayak uyduran bir e-Güvenlik müfredatı sağlayabilmeniz tavsiye edilir. Kullanılabilir hale getirildikçe yeni kaynakları kullanmaya devam edin. Müfredatı nasıl tasarladığınız ve kullandığınız kaynaklarının bazılarının bağlantılarına air ana hatları okul profiline yükleyebiliyor musunuz konusu en çok diğer okullar için faydalıdır.
- Çevrimiçi eylemlerin sonuçlarının tüm sınıflardaki öğrencilerle tartışılması mükemmeldir. Sözleşme koşullarını tam olarak anlamak için Şartlar ve Koşullar'ın okunması gerekir. Bu aynı zamanda veri gizliliği ile ilgili olabilir. Bir diğer önemli konu da telif hakkı ihlalidir. Materyalleri lütfen http://www.esafetylabel.eu/group/teacher/resource-upload kısmından da erişilebilen yükleme kanıtı aracılığıyla yükleyin.

Müfredat Dışı Etkinlikler

- İstendiğinde müfredat zamanı dışında öğrencilerinize e-Güvenlik desteği sağlamanız iyidir. Tüm öğrencilere çevrimiçi güvenlik sorunları ile başa çıkmayı desteklemeyi teklif etmeyi düşünün. Öğrencilerin alışmalarına yardımcı olmak için Facebook gizlilikleri vb. ayarlamak gibi bir "ameliyat" sağlamak yararlı olabilir. E-Güvenlik Etiketi portalı, bunun için yararlı olacak kaynakları sağlar; öğrencilerin okul dışında çevrimiçi teknolojiyi kullanımına ilişkin bilgi notunu https://www.esafetylabel.eu/group/community/pupils-use-of-online-technology-outside-school kısmından kontrol edin.

Destek Kaynakları

- e-Güvenlik konularında öğrencilerin güven duymasını sağlayacak bir eğitmen şeklinde hareket eden bilgili bir personele sahip olmanız harika.

Personel Eğitimi

- Tüm personelin e-Güvenlik konularında düzenli eğitim alması öğrencileriniz için gerçek bir fayda sağlamalıdır. Personelden eğitimin orta ve uzun vadeli faydaları hakkında geri bildirim toplamaya devam edin ve eğitim kurslarına dair önerileri görmek için https://www.esafetylabel.eu/group/community/suggestions-for-online-training-courses bölümünden e-Güvenlik Etiketi portalına başvurun.
- Okulunuz, her öğretmenin siber zorbalık konusunda eğitilmesini sağlar. Lütfen bu eğitimlerde kullandığınız materyalleri http://www.esafetylabel.eu/group/teacher/my-school-area bölümüne yükleyin. Bu eğitimin aynı zamanda vaka sayısına etkisini de izliyor musunuz?

Öğretmenlere boş zamanlarında öğrenciler tarafından kullanılan teknoloji hakkında bilgi vermeniz iyi bir uygulamadır. Bu farkındalık, okulun gücünün kapatılması meselesini ele almanın ilk adımı olduğundan önemlidir. Öğrencilerden aynı zamanda okul dışında erişimleri olmayan teknolojileri kullanarak ödev yapmaları istenmemelidir. Şu kısma da göz atmak isteyebilirsiniz:

http://essie.eun.org/

Gönderdiğiniz Değerlendirme Formu büyük bir soru havuzundan oluşturulmuştur. Ankette belirtilmeyen alanlarda e-Güvenliği iyileştirip iyileştirmediğinizi bilmemiz faydalı olabilir. Bu tür değişiklikleri e-Güvenlik portalının http://www.esafetylabel.eu/group/teacher/my-school-area bölümünden http://www.esafetylabel.eu/group/teacher/resource-upload aracılığıyla yükleyebilirsiniz. Unutmayın, kanıtların yüklenmesi, başkalarıyla olan alışverişleriniz aracılığıyla forum ve sağlanan şablonda olayları bildirmeniz de hesaba katıldığından formun doldurulması Akreditasyon Süreci'nin yalnızca bir bölümüdür.