ÇERKEZKÖY ATATÜRK İLKOKULU

Veli Olarak; Güvenli İnternet Kullanımı İçin Üzerime Düşen Görevler

Değerli Veliler;

AİLEMİZİN YENİ ÜYESİNİ TANIYIN

1. En az çocuğunuzu koruyacak kadar İnternet kullanmayı öğrenin,
2. İnternet kullanımında yasaklayıcı değil, zaman açısından sınırlayıcı olun,
3. İnternetin derslerini aksatmasına izin vermeyin,
4. Diğer sosyal aktivitelere katılımını özendirin,
5. İnternet sebebiyle sorumluluklarını yerine getirmemesine fırsat vermeyin.

OLASI TEHLİKE ve RİSKLER... DİKKAT!!!

1. Aşırı kullanımın sebep olduğu internet bağımlılığı,
2. Fiziki sağlık sorunları, (ekran başında aşırı vakit geçirmekten kaynaklı)
3. Öfke, şiddet ve yalnızlık gibi psikolojik sorunlar, (sosyal çevre yoksunluğu)
4. Şiddet ve müstehcen içerikli görüntülerin (tehlikelerini... **öğrenin!!!**

ÇERKEZKÖY ATATÜRK İLKOKULU

BİLMELERİ GEREKENLERİ ÖĞRETİN

1. İnternette tanımadıkları kişilerden gelen arkadaşlık tekliflerine hayır demeyi,
2. Hoşlanmadıkları bir durumu sizinle paylaşmaları gerektiğini,
3. İnternet üzerinden gelen cazip, fakat aldatıcı teklifleri reddetmeyi,
4. İnternetin gerçek hayattan çok farklı olduğunu,
5. Hayatın sadece İnternetten ibaret olmadığını... (öğretin)!.

ÖNCE SİZ ÖRNEK OLUN

1. İnternet kuralları belirleyin ve bunlara önce siz uyun,
2. Çocuklarınızla aranızda aile sözleşmesi imzalayın ve uygulayın,
3. Belirlediğiniz İnternet kullanım zamanına siz de riayet edin,
4. İnternet dışında aile içi aktiviteler düzenleyin,
5. Çocuğunuzun en iyi ve en güvenli limanı siz olun.

İnternetteyken sizi rahatsız eden, Zararlı ve rahatsız edici internet sitelerini www.ihbarweb.org.tr adresine ya da **0312 582 82 82** numaralı telefona hemen şikayet edin.

SOSYAL AĞLARA DİKKAT EDİN

1. Çocuğunuz bu sitelere (örn. facebook) üye ise, sizde üye olup on un arkadaşı olun.
2. Profillerindeki gizlilik ayarlarını yapmasını sağlayın.
3. Tam isim, adres, telefon, okul, özel fotoğraflarını paylaşmamasını söyleyin.
4. Tanımadıkları kişileri arkadaş listelerine eklememelerini söyleyin.
5. Arkadaşı olarak kimlerle arkadaşlık ettiğini aralıklarla kontrol edin.

Sevgili Öğrenciler;

10 Temel Kural

SANAL OYNA; GERÇEK YAŞA

1.İnternette geçirdiğin süreleri kontrol etmelisin. Hayat sadece İnternetten ibaret değildir. Arkadaşlarınla beraber gerçek hayatta da eğlenebilirsin.

2.İnternette gezinmek için evinizi ve ailenizle birlikte oturduğunuz odayı tercih edin.

3.Seçimlerinizi ailenizle ve öğretmenlerinizle beraber yapın. Onlara danışmaktan çekinmeyin. Beğendiğiniz siteleri Sık Kullanılanlar'a ekleyebilirsiniz.

4.İnternette karşılaştığınız herhangi bir bilgiyi başka kaynaklardan da sorgulayın ve doğruluğunu araştırın. Ayrıca, bir ödev hazırladığınızda, bulduğunuz bilgileri ve kullandığınız resimlerin kaynağını mutlaka belirtmelisiniz.

5.Tanımadığınız kişilerle sohbet etmeyin. Sosyal paylaşım sitelerinde kesinlikle tanımadığınız kişilerle arkadaş olmayın. Yeni arkadaşlar edinmek eğlenceli olabilir ancak unutmayın ki bazıları kendileri hakkında yalan söyleyebilir.

6.İnternet ortamında tanıştığın bir yabancıyla gerçek hayatta buluşmamalısın. Gerçekten tanışmak istediğin biri olursa yanında mutlaka aile bireylerinden bir yetişkin olmalı ve buluşmak için kalabalık yerleri tercih etmelisin.

7.İnternet ortamında kişisel ve özel bilgilerinizi vermeyin. Kullanılan şifreler hiçbir şekilde başkalarıyla paylaşılmamalı, kolay elde edilebilecek yerlere yazılmamalı. Verdiğiniz ufak gibi görünen bilgiler bile kötü niyetli kişiler tarafından kullanılabilir.

8.Tanımadığınız kişilerden gelen mesajları asla açmamalısınız. Çünkü bunlar genellikle uygunsuz, virüslü ya da gereksiz şeyler içermektedir. Bunlara karşı bilgisayarınızda mutlaka güncel bir anti-virüs ve güvenlik programı bulunmalıdır.

9.Size yapılmasını istemediğinizi başkalarına da yapmayınız. Kimseye hakaret, argo, küfürlü hitap etmemelisiniz. Yüzüne söylemek nasıl saygısız bir hareketse internet üzerinden yapmak da öyledir.

10.İnternet ortamında sizi rahatsız eden şeylerle (kişilerin küfürlü ve argo konuşmaları, hakaretler, uygunsuz teklifler ya da zararlı sitelerle) karşılaştığınızda ailenize, öğretmenlerinize ya da İhbarweb'e (www.ihbarweb.org.tr) şikayet edebilirsiniz.

Sosyal Ağ Kullanırken

1. Kişisel bilgilerinizi herkesle paylaşmamanızı tavsiye ederiz.

- Telefon numaranız.
- Ev, okul ve iş adresiniz.
- Doğum gününüz, yaşınız.
- T.C. kimlik numaranız.
- E-mail adresiniz.

2. Paylaştıklarınız şeyleri istemediğiniz kişilere kapatın.

- Gönderilerinizi.
- Ailenizle ilgili bilgilerinizi.
- İlgilendiklerinizi.
- Dini inanç ve siyasi görüşünüzü.
- Bulunduğunuz yeri.
- Size ait fotoğraf ve videolarınızı.

3. Tanımadığınız kişilerin arkadaşlık tekliflerini reddedin. Çünkü

- Tanımıyorsunuz.
- Niyetini bilmiyorsunuz.
- Zarar görebilirsiniz.
- Üzülebilirsiniz.

4. Güçlü şifreler oluşturun ve şifrenizi kimseyle paylaşmayın. Çünkü

- Sizin adınıza arkadaşlarınıza mesaj gönderebilirler, zor durumda kalırsınız.
- Profilinizde sizin istemediğiniz şeyleri paylaşabilirler.

ÇERKEZKÖY ATATÜRK İLKOKULU İLKOKULU

VELİ –ÖĞRENCİ BİLGİLENDİRME BROŞÜRÜ

Güvenli İnternet Kullanımı

1.Sayfa

eSafety Label - Action Plan

Action plan submitted by Esra AK for Çerkezköy Atatürk İlkokulu - 05.12.2020 @ 19:16:10

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

- It is important that your ICT services are regularly reviewed, updated and removed if no longer in use. Installing the latest versions and patches often addresses security vulnerabilities without which your services might come under attack. Ensure that this is part of the job description of the ICT coordinator.

- 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 very good that all your school devices are virus protected. Make sure you also have included a paragraph on virus protection in both your school policy and your Acceptable Use Policy, and ensure that staff and pupils rigorously apply school guidelines. If you need further information, check out the fact sheet on Protecting your devices against malware at www.esafetylabel.eu/group/community/protecting-your-devices-against-malware.

Pupil and staff access to technology

- Since staff and pupils can use their own equipment on your school network, it is important to make sure that the Acceptable Use Policy is reviewed regularly by all members of the school and adapted as necessary. It must be discussed with pupils at the start of each academic year so that they understand what is in place to protect them and their privacy, and why. Base the policy around behaviour rather than technology. Visitors must also read and sign the Acceptable Use Policy before they use the school’s network.

- Consider whether banning mobile devices is a rule that is fit for purpose and if your school might want to allow digital devices for some class activities.You could develop as part of your Acceptable Use Policy a section on how digital technologies can and cannot be used in the classroom; see the fact sheet on Using Mobile Phones at School (www.esafetylabel.eu/group/community/using-mobile-device-in-schools).

Data protection

- 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.

- You have a good policy of encrypting pupil data and storing it safely. Ensure all new staff made aware of the procedures for encryption and data handling and that there is a named point of contact acting as the data controller for your school. Upload to your school profile some guidelines about protecting sensitive data through an encryption system so that other schools can benefit from your experience.

- 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.

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 is good that you can produce an overview of installed software and their licences in a short time frame with the help of several people. Consider centralising this.

IT Management

Policy

Acceptable Use Policy (AUP)

- 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

- Are all staff familiar with the procedure for dealing with material that could potentially be illegal? Is there a named person from the school senior leadership team who takes overall responsibility in this type of case? The procedure needs to be clearly communicated to all staff in the School Policy, and to staff and pupils in the Acceptable Use Policy. Remember to report and suspected illegal content to your national INHOPE hotline (www.inhope.org).

- Ensure that all staff, including new members of staff, are aware of the guidelines concerning what to do if inappropriate or illegal material is discovered on a school machine. Ensure, too, that the policy is rigorously enforced. A member of the school's senior leadership team should monitor this.

Staff policy

- New technologies, such as smartphones or other mobile devices bring a new set of risks with them. Ensure that your teachers are aware of those. This way they can avoid the pitfalls when using the devices and also pass the knowledge onto the pupils.

- You have guidelines in your Acceptable Use Policy (AUP) on teachers' classroom usage of mobile phones. Upload your AUP to your school profile as it is a model of good practice that can help other eSafety Label schools.

- Ensure that all staff, including new members of staff, are aware of the policy concerning online conduct. This should be a topic that is regularly discussed at staff meetings and clearly communicated in the School Policy, and to staff and pupils in the Acceptable Use Policy. Regularly review and update both documents as necessary.

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.

- You have defined electronic communication guidelines in your Acceptable Use Policy and this would be a useful example of good practice for other schools. Can you create a tutorial about electronic communication guidelines for pupils and upload it to your school profile via your My school area so that other schools can benefit from your experience.

School presence online

- It is good that pupils can give feedback on the school's online presence. Think about creating a space that is entirely managed by pupils. It's a great opportunity to learn about media literacy and related issues. It also can help to establish a peer network of support. Find out more about in the eSafety Label fact sheet.

- 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.

Practice

Management of eSafety

- Ensure that the governor or board member appointed for eSafety has the opportunity to receive regular training and also to ensure that colleagues are aware of eSafety issues. Involve your governing body in the development and regular review of your School Policy. See our fact sheet on School Policy www.esafetylabel.eu/group/community/school-policy.

eSafety in the curriculum

- It is good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.

- It is good practice that all pupils in all year groups in your school are taught about eSafety. It continues to be important to review regularly the curriculum provision to ensure it meets ever-changing needs. If you have a curriculum review process of this kind, it would be helpful to other schools if you could publish this on your school profile. To upload go to your My school area.

- Sexting is an issue which affects many young people. Sharing possible consequences and risks with them is important, as is the opportunity for some discussion around the issue. Sexting should be part of a broad and balanced eSafety curriculum.

- It is good that you are making a specific reference to sexting within your child protection policy as this is a growing issue that many young people are having to deal with. It is also important to ensure that you are providing appropriate education for pupils about this issue.

- It is very good that, in your school, pupils are taught from an early age on about responsibilities and consequences when using social media. Please share any resources through the uploading evidence tool, accessible also via the My school area.

Extra curricular activities 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.

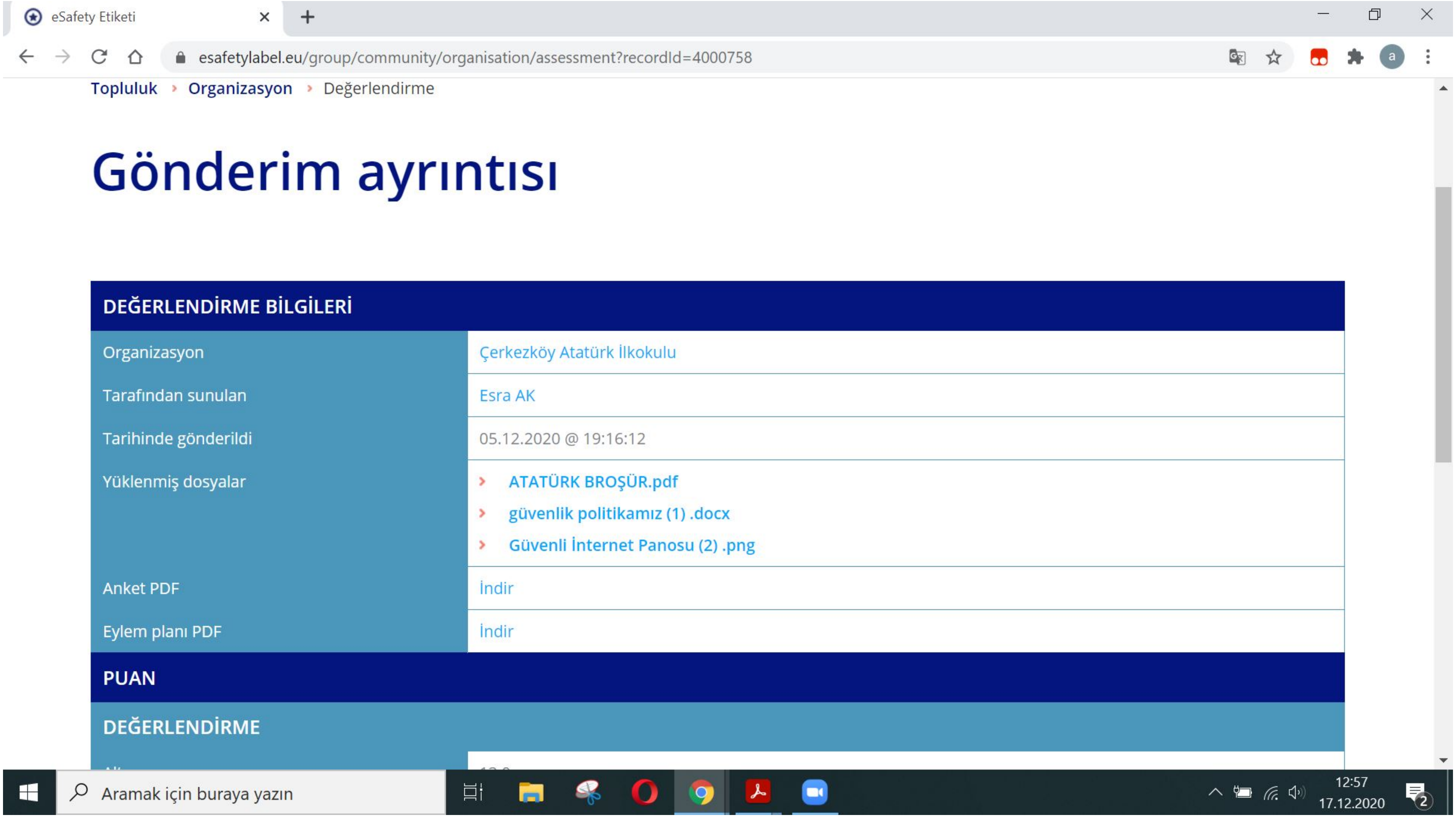
- It is good to know that other school services are involved in eSafety issues (e.g. counsellors, psychologists, school nurse). Are they also invited to contribute to developing and regular review of your School Policy? Publish a case study about how this is managed in your school on your school profile page on the eSafety Label project website, so that others can learn from your experience.

Staff training

- 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 Etiketi
esafetylabel.eu/group/community/organisation/assessment?recordId=4000758
Aramak için buraya yazın
12:57
17.12.2020

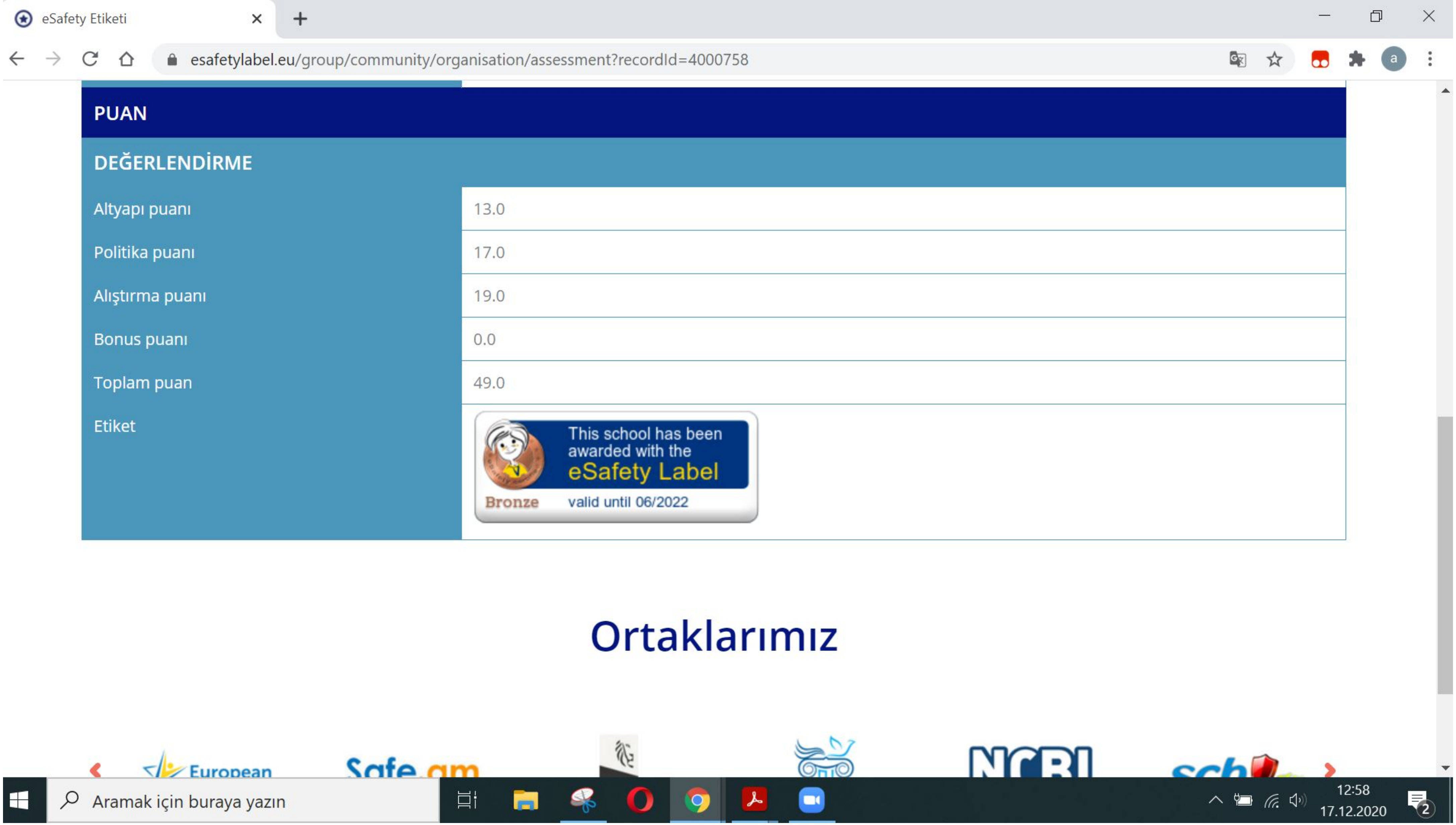
Topluluk › Organizasyon › Değerlendirme

Gönderim ayrıntısı

DEĞERLENDİRME BİLGİLERİ	
Organizasyon	Çerkezköy Atatürk İlkokulu
Tarafından sunulan	Esra AK
Tarihinde gönderildi	05.12.2020 @ 19:16:12
Yüklenmiş dosyalar	› ATATÜRK BROŞÜR.pdf › güvenlik politikamız (1) .docx › Güvenli İnternet Panosu (2) .png
Anket PDF	İndir
Eylem planı PDF	İndir

PUAN

DEĞERLENDİRME



esafetylabel.eu/group/community/organisation/assessment?recordId=4000758

PUAN

DEĞERLENDİRME

Altyapı puanı	13.0
Politika puanı	17.0
Alıştırma puanı	19.0
Bonus puanı	0.0
Toplam puan	49.0
Etiket	This school has been awarded with the eSafety Label Bronze valid until 06/2022

Ortaklarımız

Aramak için buraya yazın
12:58
17.12.2020

This school has been awarded with the

eSafety Label

Bronze

valid until 06/2022