MENTEŞE ŞEHİT İBRAHİM KARAOĞLANOĞLU ORTAOKULU

E-GÜVENLİK POLİTİKASİ

Bu e-güvenlik politikası bakanlığımızın 2017/12 sayılı genelgesinde yer alan kurallara ve okulumuz öğretmenler kurulunda alınan kararlara istinaden hazırlanmış olup,tüm okul personeline internet kullanımının okul etiğine ve yasaya uygun olması gerektiğini hatırlatır.

ŞEHİT İBRAHİM KARAOĞLANOĞLU ORTAOKULU

E-Güvenlik Politikası

Bu e güvenlik politikası bakanlığımızın 2017/12 sayılı genelgesi'n de yer alan kurallara ve okulumuz öğretmenler kurulunda alınan kararlara istinaden hazırlanmış olup tüm okul personeline , internet ve akıllı tahta kullanımının, diğer uygun politikalara ve yasaya uygun olması gerektiğini hatırlatmaktadır.

- Öğrencilerin korunması için hazırlanan e-güvenlik politikamız, tüm okul personeli (öğretmen, idareci ve yardımcı personel) için geçerli olup, veri ve veri depolama, çevrimiçi ve çevrimdışı iletişim teknolojileri erişim cihazlarını içerir. Örneğin:cep telefonları,tabletler,sınıflardaki etkileşimli tahtalar,dijital kameralar, e-posta ve sosyal medya siteleri.

- İdareci,öğretmen,okul personeli kullanımı için sağlanan donanım ve yazılımları yalnızca personel üyeleri tarafından ve yalnızca eğitim amaçlı kullanılabilir. Sistemlere veya kişisel verilere yetkisiz erişimi önlemek için, ilk çıkışı yapmadan veya giriş bilgilerinizi uygun bir şekilde kilitlemeden herhangi bir bilgi sistemini gözetimsiz bırakmayınız.

- Öğretmenlerin ,okul personelinin,öğrencilerin ve anne baba kişisel verilerinin Veri Koruma Yasası'na uygun olmasını sağlayınız. Bu, tüm kişisel verileri, uygun güvenlik önlemleri alınarak özel ve güvenli tutunuz. Öğrencilerin katıldığı tüm etkinliklerde veli izin diekçesi alınız.Öğrencilerin resim ,video ve ses kayıtlarını sadece bakanlığımızın 2017/12 sayılı genelgesinde belirtildiği şekilde kullanınız ve mutlaka veli izin diekçesi alınız.

- Öğrencilerinizin yüzleri belli olacak şekilde fotoğraf yada olabildiğince öğrencilerin yüzlerinin seçildiği fotoğraf ve videoların paylaşımından kaçınılması,

- Video ve resmilerin Youtube ve Vimeo'da kısıtlamalar ile paylaşılması. video görüntülerini, Adı soyadı ,yaşı gibi kimlik bilgilerini paylaşmayınız.

- Okulun bilgisayar sisteminde, kişisel fotoğraflar, dosyalar veya finansal bilgiler gibi okul faaliyetleriyle ilgisi olmayan kişisel bilgileri saklamayınız,

- Öğrencilerin çevrimiçi güvenliğiyle ilgili tüm endişeleri, okul idaresine ve sınıf rehber öğretmenine en kısa sürede bildiriniz,

- Okulun koyduğu filtreleme ve / veya güvenlik sistemlerini atlamaya çalışmayınız . Bir bilgisayarın veya sistemin virüs veya diğer kötü amaçlı yazılımlardan zarar gördüğünden veya etkilenmediğinden veya okulla ilgili belgeleri veya dosyaları kaybettiğinizi düşünüyorsanız, bunu mümkün olan en kısa sürede okul idaresine bildiriniz,

- Sistem güvenliğine dikkat ediniz ve şifre veya güvenlik bilgilerini ifşa etmeyiniz. 'Güçlü' bir şifre kullanınız (güçlü bir şifre, 8 veya daha fazla karakter içeren, harfler ve semboller içerir, sözlük kelime içermez ve sadece bir sistemde kullanılır).

- İdarenin izni olmaksızın, tarayıcı araç çubukları veya donanım da dahil olmak üzere, satın alınan veya indirilen herhangi bir yazılımı yüklemeye çalışmayınız.

- Eğer eğitim amaçlı video konferans çalışması yapacaksanız önce okul idaresinden izin alınız ve ailelerden veli izin belgesi alınız.

- İnternet erişim ağımız meb tarafından güvenle korunmaktadır , çevrimiçi olmayan hazır egitimi metaryelleri kullanıyorsanız öğrenci yaş grubuna ,eğitim-öğretim müfredatlarına uygunluğuna dikkat ediniz.Tüm sorumluluk size aittir.

- Telif hakkı ve fikri mülkiyet haklarına saygı duyunuz.

- Okulumuz öğretmenleri , kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim almış olup e güvenlik konusunda tereddütleri olan öğretmenler Bt öğretmenimizden yardım alabilirler.

- E- güvenlik ile ilgili dökümanlara okul web sitemizdeki ilgili liklerden ulaşabilirsiniz.

Okulda Kişisel Cihazların ve Cep Telefonlarının Kullanımı
(idareci ,öğretmen, pesonel)

Cep telefonlarının ve kişisel cihazların çocuklar, gençler ve yetişkinler arasındaki yaygın bir şekilde kullanılmasi, çevrimçi ve çevrimdışı kullanımlarda siber zorbalık, sakıncalı sitelere erişim v.b. tehlikelere açık olması sebebiyle Şehit İbrahim Karaoğlanoğlu Ortaokulu olarak güvenlik önlemleri almamız kaçınılmazdır.

- Okula getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir. Okul, bu tür öğelerin kaybı, çalınması veya zarar görmesi konusunda sorumluluk kabul etmez. Okul, bu tür cihazların potansiyel veya fiili neden olduğu olumsuz sağlık etkileri için sorumluluk kabul etmez.

- Öğretmenler, kişisel telefonların ve cihazların herhangi bir şekilde kullanımının daima veri koruma ve ilgili okul politikası ve prosedürleri uyarınca yerine getirilmesini sağlayacaktır

- Kişisel cep telefonlarınızı ve cihazlarınızı ders saatlerinde kapatılıp / sessiz moda alınız.

- Derslerde öğrencilerin telefonlarını (eğer ders metaryeli olarak kullanılmayacaksa) müdür yardımcısının odasındaki çekmeceye koymalarını sağlayınız.

- Öğretmenler,idareceler bütün derslerde(branşlarda) müfredat boyunca uygun olduğu yerlerde sosyal medya kullanımı,internet etiği,çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi riskler ve alınacak tedbirlerle ilgili, öğrencileri bilgilendirir.

Öğrencilerin kişisel cihazlarını ve cep telefonlarını kullanımı

- Öğrenciler, kişisel cihazların ve cep telefonlarının Siber zorbalık sosyal medyanın bilinçli ve güvenli kullanımı konusunda İ öğretmenimiz tarafından verilen eğitimi alacaklardır.

- Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.

-Cep telefonları veya kişisel cihazlar, müfredat tabanlı etkinlik kapsamında ders öğretmenin onayı alınarak kullanılabilir.

- Öğretmenin izni olmadan kullanılan telefon yada kişisel cihaz öğretmen tarafından okul idaresine teslim edilir ve idare tarafından öğrenci velisine teslim edilir.

- Öğrenciler okulun resmi vifi ağına bağlanabilir.

- *Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul telefonunu kullanmasına izin verilecektir.*

- *Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vermelidirler.*

- *Öğrencinin kişisel cihazında veya cep telefonunda bulunan materyalin yasadışı olabileceği veya cezai bir suçla ilgili kanıt sağlayabileceğinden şüpheleniliyorsa, okul idaresine bildirilir ve gerekli idari işlemler yapılır.*

- *Öğrenciler öğretmeninin izni olmadan okula telefon getiremez ,kullanamaz*

- *Okula getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir. Okul, bu tür öğelerin kaybı, çalınması veya zarar görmesi konusunda sorumluluk kabul etmez.*

Veliler ve ziyaretçilerin kişisel cihazların ve cep telefonlarının kullanılması

- Ebeveynler ve ziyaretçiler, okulun kabul edilebilir kullanım politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.

- Fotoğraflar veya videolar çekmek için ziyaretçiler ve ebeveynler tarafından cep telefonlarının veya kişisel cihazların kullanılması, okul resim kullanımı politikasına uygun olarak gerçekleştirilmelidir.

-Personel uygun olmayan ve güvenlik ihlali olduğunda her zaman ziyaretçilerin herhangi bir ihlalini idareye bildirecektir.

Okulumuzun yaptığı e-Güvenlik çalışmaları ve Personel Eğitimi

- Okulun tüm üyeleri, cinsel içerikli mesajlaşma, çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi riskler ve alınacak tedbirlerle ilgili, Muğla İl Milli Eğitim

Müdürlüğü tarafından “Fatih Projesi Bilişim Teknolojilerinin ve İnternetin Bilinçli,Güvenli Kullanımı” semineri almıştır.

- Okulumuz eTwinning proje ekibi öğretmenleri ebaonline eğitimler http://etwinningonline.eba.gov.tr/ portalinde çevrimiçi Güvenli İnternet kursuna katılmışlardır.

- Okulumuzda her yıl Şubat ayında Güvenli İnternet Günü etkinlikleri yapılarak öğretmen ve öğrencilerimizde farkındalık yaratılır.

- *Okulumuz daha güvenli bir okul için ESAFERTYLABEL.EU’ den* ***Saferty Bronz Etiketi*** almıştır.

- Öğrencilerimize Siber zorbalık,internet etiği,sosyal medya kullanımı konularında Güvenli İnternet eğitimi verilmektedir.

- İngilizce öğretmenimiz tarafından akran zorbalığı ve internet bağımlılığı konusunda öğretmen,idareci ve öğrenci bilgilendirme farkındalık yaratma seminerleri verilmiştir.

- Sorunları çözmek için ebeveynlerin ve öğrencilerin okulla ortak çalışması gerekir.

OKUL MÜDÜRÜ
ÇAĞDAŞ ÇELİKÖZ

eSafety Label - Action Plan for: Muğla/Menteşe Şehit İbrahim Karaoglanoglu Ortaokulu

Assessment form was submitted by: seval gegez - 2018-02-28 13:57:15

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 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/teacher/protecting-devices-against-malware.
- You have differentiated levels of filtering in your school which is an excellent policy. A good policy still needs to be regularly updated - is the system being regularly updated? How often are sites requested to be blocked or unblocked? Periodically evaluate whether it is fit for purpose and involve all stakeholders in this process.
  In addition, bear in mind that 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.

Pupil and staff access to technology

- 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/teacher/removable-devices to make sure you cover all security aspects.
- It is great that in your school laptops/tablets are easily accessible within a lesson. Using them provides best practise for pupils in dealing with new media. Ensure that safety issues are also discussed.

Data protection

- You have a good policy of keeping your learning and administration environments separate. It is good to ensure that staff training on managing these environments is up to date as you continue to review your policies. Share your policy with other eSafety Label users by uploading it to your school profile.
- 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/teacher/safe-passwords.
  Include these rules in your Acceptable User Agreement and avoid giving new users a standard "first access" password.