MALATYA BİLİM VE SANAT MERKEZİ

e Güvenlik Stratejik Planı

e Twining Okulu Stratejik Planı

2021

İÇİNDEKİLER

GİRİŞ ve PLAN HAZIRLIK SÜRECİ

2019-2023 dönemi e güvenlik stratejik plan hazırlanması süreci web güvenlik komisyonunun oluşturulması ile başlamıştır. Ekip tarafından oluşturulan çalışma takvimi kapsamında ilk aşamada durum analizi çalışmaları yapılmış ve durum analizi aşamasında paydaşlarımızın konu ile ilgili bilgi düzeyini ölçmek üzere anket, toplantı ve görüşmeler yapılmıştır.

Durum analizinin ardından geleceğe yönelim bölümüne geçilerek okulumuzun amaç, hedef, gösterge ve eylemleri belirlenmiştir. Çalışmaları yürüten ekip ve kurul bilgileri altta verilmiştir.

MALATYA BİLİM VE SANAT MERKEZİ E-GÜVENLİK KURULU			
S.NO	ADI SOYADI	GÖREVİ	SORUMLULUK ALANI
1	Ümit Arslan	Kurum Müdürü	E Güvenlik ile ilgili yasal mevzuat sorumlusu
2	Arif Akça	Müdür Yardımcısı	İnternet Sayfası Sorumlusu
4	Ramazan Berkeban	Rehber Öğretmen	Öğrenci ve Veli Bilgilendirme Sorumlusu
5	Serdar Mutlu	Bilişim Teknolojileri Öğretmeni	E Güvenlik Okul Sorumlusu
6	Zuhal Ayik Yıldırım	İngilizce Öğretmeni	Öğretmen Bilgilendirme Sorumlusu
7	Okay Demir	Müdür Yardımcısı	üye

OKULUN DEĞERLERİ

- Tüm paydaşlarımızı çevrimiçi olarak korumak ve güvenliklerini sağlamak
- Teknolojinin potansiyel riskleri ve yararları konusunda tüm paydaşların farkındalığını sağlamak
- Güvenli internet kullanırken tüm olumlu davranışları https://www.esafetylabel.eu/home da online modellemek ve kendi standartlarını ve uygulamalarını yürütme gereksinimini fark etmek
- Her türlü bilinen çevrimiçi güvenlik sorunlarına yanıt verebilecek prosedürleri tanımlamak

SWOT Analizi

Okulumuzda çevrim içi güvenlik hizmetlerini geliştirerek öğrencilerimizi, velilerimizi ve personelimizi her türlü bilinen tehditlerden korumak, onlara karşı önlem almak ve yaşadıkları olumsuzlukları çözmek için strateji geliştirmelerini sağlamak amaçlanmıştır.

Öğretmenler, okul web sitesi, görüntü ve video paylaşımı, kullanıcılar, içerik, internet ve bilişim cihazları kullanımı, cep telefonu ve kişisel cihaz kullanımı hakkında kurallar belirlenmiştir. Bu kurallar detaylı olarak **Malatya Bilim Ve Sanat Merkezi e güvenlik politikasında** açıklanmıştır.

	Güçlü Yönler	Zayıf Yönler
İç Faktörler	1. Öğretmenlerin e güvenlik konusunda ilgili olması 2. Öğretmenlerin teknolojiyi etkin kullanması 3. Okulumuzda teknoloji bakımından yeterli olması 4. Okulumuzda müfredatlımızda e güvenlik konusunun işlenmesi 5. Okulumuzda Kabul Edilebilir Kullanım Politikasının olması	1. Velilerin e güvenlik hakkında bilgilerinin olmaması 2. Sürekli göç alan bir okul olunmasından dolayı veli profilinin sürekli değişmesi 3. Velilerin sosyoekonomik durumunun zayıf olması
External factors (Aspects outside the control of your school	**Fırsatlar**	**Tehditler**
	1. Milli Eğitim Bakanlığı'nın e güvenlik ile ilgili kendi filtreleme sisteminin olması 2. Çevrim içi filtreleme sisteminin okul bilgisayarlarımızda yüklü olması ve sürekli güncellenmesi 3.Öğrencilerinin yaşlarının küçük olması okulda öğretmenlerinin gözetiminde teknolojiyi kullanması.	1. Öğretmenlerimizin kişisel bilgisayarlarının yeterli çevrim içi güvenlik kaynaklarının olmaması 2. Öğrencilerin yaş grubunun küçük olması ve bu yüzden tehditlerin farkında olmaması 3.Velilerimizin eğitim düzeyinin düşük olması

ÇEVRİM İÇİ GÜVENLİK STRATAJİSİNİ TANIMLAMA

Strateji Vizyonu

Okulumuz, teknolojik aletleri kullanırken çocukları ve yetişkinleri dijital dünyanın zararlarından korumaktır. Bunun için gerekli çalışmalar yapılmaktadır. Sanal platformların ve bilgi iletişim teknolojilerinin vazgeçilmez hale geldiğini görülmektedir. Çocuklarımızı bu ortamlardan gelebilecek riskleri yönetmeleri, bu risklere nasıl tepki vermeleri konusunda strateji geliştirmenin yollarını öğrenmeleri amaçlanmıştır. Personelimizin mesleki çalışmalarını desteklemek, başarıyı teşvik etmek ve yönetim işlevlerini geliştirmek için internet erişimi sunma yükümlülüğü verilmiştir. Bütün paydaşlarımızı (velilerimizi, öğrencilerimizi ve personelimizi) sanal ortamdan korunmasını sağlama misyonumuzdur.

Odak Noktası

1. Sosyal medya ile ilgili riskler konusunda okul farkındalığının artması
2. e güvenliğin öneminin farkına varılması
3. Öğrencilerimizi siber zorbalığa, cinsel içerikli mesajlara karşı korunması ve strateji geliştirilmesinin sağlanması
4. Personelin kendi e güvenliği hakkında bilgilendirilmesi

STRATEJİK HEDEFLER VE AMAÇLAR

TEMA IV: e Güvenlik

Stratejik Amaç 4: Okulumuzu e Twining okulu yapmak

Stratejik Hedef 4.1. Okulumuzun e Twining okulu olması için gerekli iş ve işlemlerin yapılması

Performans Göstergeleri

NO	PERFORMANS GÖSTERGESİ	MEVCUT	HEDEFLER	
		2021	2022	2023
PG.4.1.a	E twining projelerinin yapılması	2	3	6
PG.4.1.b	Komisyon üyelerinin eğitimlere katılımının sağlanması		2	3
PG.4.1.b	E güvenlik komisyonunun oluşturulması		X	X

Eylemler

No	Eylem İfadesi	Eylem Sorumlusu	Eylem Tarihi
4.1.1	Personelimizi http://etwinningonline.eba.gov.tr/ da eğitimleri almasını sağlamak	İngilizce Öğretmeni	Her ay
4.1.2	Komisyon üyelerinin eğitimlere katılımının sağlanması	Okul Müdürü	2023
4.1.3	E güvenlik komisyonunun oluşturulması		2022

Stratejik Amaç 5: internetin her ortamda Güvenli internet kurallarına uygun kullanımının artırılması

Stratejik Hedef 5. 1. Okul web sitesi amaca uygun, güvenli, aktif ve güncel olarak kullanılacaktır.

Performans Göstergeleri

NO	PERFORMANS GÖSTERGESİ	MEVCUT	HEDEFLER	
		2021	2022	2023
PG.5.1.a	Okul web sitesinde yayınlanan haber ve duyuru sayısı (sayı)	40	45	50
PG.5.1.b	Okul web sitesinde yer alan haberlerin görüntülenme sayısı (sayı)	200	250	300
PG.5.1.c	Okul web sitesinde yer alan haberlerin ve görüntülerin güvenli internet kapsamında paylaşım oranı (%)	70	75	80

Eylemler

No	Eylem İfadesi	Eylem Sorumlusu	Eylem Tarihi
5.1.1	Okul web sitesine aylık bültenler düzenli olarak eklenecektir.	Müdür yardımcısı	Her ay
5.1.2	Okul web sitesine veli toplantıları, rehberlik servisi seminerleri duyuru olarak girilecektir.	Müdür yardımcısı	Her ay
5.1.3	Okulda yapılan etkinlik ve çalışmaların fotoğrafları güvenli internet kapsamında veli izin onayı alınarak düzenli olarak okul web sitesinde yayınlanacaktır.	Müdür yardımcısı	Her Hafta
3.3.4	Velilere kısa mesaj yolu ile okul web sitesinin takibi hatırlatılacaktır.	Müdür yardımcısı	Periyodik aralıklarla

Stratejik Hedef 5. 2: Sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması.

Performans Göstergeleri

NO	PERFORMANS GÖSTERGESİ	MEVCUT	HEDEFLER	
		2021	2022	2023
PG.5.2.a	Velilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması (%)	20	25	30
PG.5.2.b	Öğrencilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması (%)	40	45	50
PG.5.2.c	Personelimize sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması (%)	40	45	50

Eylemler

No	Eylem İfadesi	Eylem Sorumlusu	Eylem Tarihi
5.2.1	Konu ile ilgili öğrenci personel ve velilere Seminerler vermek	Rehber öğretmenler	Her ay
5.2.2	Broşürler dağıtmak	Web güvenlik komisyonu	Her ay

Stratejik Hedef 5.3 e güvenliğin öneminin okul farkındalığını her yıl %10 artırmak

Performans Göstergeleri

NO	PERFORMANS GÖSTERGESİ	MEVCUT	HEDEFLER	
		2021	2022	2023
PG.5.3.a	Velilerimize e güvenlik konusunda bilgilendirme yapma %	20	30	40
PG. 5.3.b	Öğrencilerimize e güvenlik konusunda okul farkındalığının arttırılması	30	40	50
PG. 5.3.c	Personelimize e güvenlik konusunda okul farkındalığının arttırılması	40	50	60

Eylemler

No	Eylem İfadesi	Eylem Sorumlusu	Eylem Tarihi
5.3.1	Konu ile ilgili öğrenci personel ve velilere Seminerler vermek	Rehber öğretmenler	Her ay
5.3.2	Pano hazırlamak	Sınıf öğretmenleri	Her ay
5.3.3	personelimizi https://www.esafetylabel.eu /home a üye olmasını sağlamak	Öğretmenler kurul toplantısı	2022

Stratejik Hedef 5.4 Öğrencilerin siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini artırmak

Performans Göstergeleri

NO	PERFORMANS GÖSTERGESİ	MEVCUT	HEDEFLER	
		2021	2022	2023
PG.5.4. a	Öğrencilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve karşı strateji geliştirmesini arttırılması	10	20	30
PG.5.4.b	Velilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini arttırılması.	50	60	70
PG.5.4.c	2021 yılının sonuna kadar personellerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini arttırılması.	60	70	80

Eylemler

No	Eylem İfadesi	Eylem Sorumlusu	Eylem Tarihi
5.4.1	İlgili konuları müfredatın içinde işlemek (Yıl içinde derslerde bu konu ile ilgili bilgilendirme, drama yapma)	Sınıf öğretmenleri	Her ünitede
5.4.2	Yıl içinde veli toplantılarında bu konu ile ilgili bilgilendirme yapma	BT rehber öğretmen	Veli Toplantıları

Stratejik Hedef 5.5 Personelin kendini e güvenliğini hakkında bilgilendirilmesinin her yıl artırılması

Performans Göstergeleri

NO	PERFORMANS GÖSTERGESİ	MEVCUT	HEDEFLER	
		2021	2022	2023
PG.4.2.a	https://www.esafetylabel.eu/home a üye olmasını sağlamak		X	
PG.4.2.b	Personelimizi http://etwinningonline.eba.gov.tr/ da eğitimleri almasını sağlamak	X	X	

İLERLEMEYİ İZLEME VE ÇEVRİMİÇİ GÜVENLİK STRATEJİSİNİ DEĞERLENDİRME

İlerleme Yada Amaç Nasıl Değerlendirilecek	Zaman Aralığı
İlk Anket yapılması (Ön değerlendirme)	2021
Son Anket yapılması (Son değerlendirme)	2023
Sınıf öğretmenlerinin ve rehber öğretmenlerinin bu konu ile ilgili yaptığı görüşmeler ve gözlemler yıl sonunda değerlendirilmesi	Her dönem sonunda
https://www.esafetylabel.eu/home a üyelik ve http://etwinningonline.eba.gov.tr/ "İnternet Güvenliği ve e Twinning Etiği" ile "eSafety Label Hakkında Herşey" eğitimlerinin sertifikaları	2022 sonuna kadar eğitimlerin tamamlanması

RİSK DEĞERLENDİRMESİ

Güvenlik Açısından Potansiyel Riskler	Belirlenen Potansiyel Riskler Nasıl Hafifletilir?
1. Öğrencinin kişisel bilgilerinin çalınması	- Öğrencinin öğretmenine bildirmesi - Öğrencinin rehber öğretmen ile görüşmesinin sağlanması - Rehber öğretmenle birlikte sınıf öğretmeninin veliye bu konu hakkında bilgilendirmesi ve nesil önlemler alabileceği hakkında görüşme yapılması -Öğretmenin web güvenlik komisyonuna bildirmesi. - Okul polisine haber verilmesi
2. Öğrencinin öğretmenin açık olan bilgisayarından e okula girip bütün notların değiştirmesi	-Öğretmenin bilgisayarına şifre koyması -Sınıftan çıkarken bilgisayarını kapatması veya uyku moduna alması -Şifresini herhangi bir yere yazmaması - Şifrelerini 3 ayda bir değiştirmesi
3. Öğrencilerin okul internet ağı kullanıcı şifresinin öğrenciler tarafından keşfedilmesi	Velilerimizi uygun bir dille bunun yanlış olduğunu anlatılır. -Uzun şifrelerin belirlenmesi -Şifrelerde büyük küçük harf, sayı ve noktalama işaretlenin kullanılarak zorluk seviyesini arttırmak -Şifrelerin 3 ayda bir değiştirilmesi