e-Güvenlik (e-Safety) POLİTİKASI

ŞEHİT SERHAT SIĞINAK MESLEKİ ve TEKNİK ANADOLU LİSESİ

e-Güvenlik (e-Safety) POLİTİKASI ve AMAÇLARI

Değişen ve gelişen teknoloji imkanlarıyla birlikte güvenlik sorunlarının nasıl aşılacağı ve teknolojiden üst düzeyde nasıl faydalanılacağı konusunda bilgilenmek, öğrencilerimizi bilgilendirmek önemli bir konu olarak karşımıza çıkmaktadır. Bu nedenle, her okulun Okul Güvenlik Politikası' na sahip olması önemli görülmektedir. Biz Güvenli İnternet Okul Politikasına sahip bir okuluz.

A. E-GÜVENLİK (E-SAFETY) POLİTİKAMIZ:

1. Okulumuzun web sitesi, instagram hesabı gibi sosyal ağları bulunmaktadır. Bu ağların üzerinde yayımlanan veriler yönetici ve editör kontrolü ile paylaşılmaktadır.

2. Okulumuzda cep telefonları ders esnasında kapalı konumda tutulmakta, eTwinning projesi yapan öğretmenler proje çalışmaları amacıyla gerektiği takdirde kullanmaktadır.

3. Rehberlik servisi tarafından, sınıflara düzenli olarak, BİT bağımlılığı, BİT'nin doğru ve güvenli kullanımı, Siber Zorbalık gibi konularda seminerler tertiplenmektedir.

4. Okulumuzda BİT doğru ve güvenli kullanımı ile ilgili sabit panolar bulunmaktadır.

5. Okulumuzun BİT laboratuvarlarında tüm öğrenciler için uyarıcı ve bilgilendirici levhalar bulunmaktadır.

6. Okulumuzun öğretmenleri Milli Eğitim Bakanlığı tarafından verilen Siber Zorbalık, BİT 'in doğru ve güvenli kullanımı gibi uzaktan ve yüz yüze eğitimler almıştır.

7. Okulumuzda "Daha Güvenli İnternet Günü" kutlanmaktadır.

8. Okulumuzun internet sitesinde e-güvenlik konusunda, https://www.guvenlicocuk.org.tr/ sitesi linki yer almaktadır. Okul paydaşlarımız istedikleri zaman konu ile ilgili bilgi alabilmekteler.

9. Rehber Öğretmenlerimiz ve bilişim teknolojileri alan öğretmenlerimiz internet etiği ve güvenli internet kullanımı konuları hakkında öğrencilerimize bilgilerini aktarmaktadır.

10. Okulumuzda 21.yy iletişim becerileri önemsenmektedir. Bununla ilgili olarak öğrencilerimizin BİT kullanım becerilerini geliştirme çalışmaları yapılmaktadır.

11. Okulumuzda Dijital vatandaş olma konusunda paydaşlarımızı bilinçlendirme çalışmaları yapılmaktadır.

B. OKULUMUZDA E-GÜVENLİK POLİTİKASININ AMACI:

- Okulumuzun tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
- Teknolojinin potansiyel riskleri ve yararları konusunda Şehit Serhat Sığınak Mesleki ve Teknik Anadolu Lisesi idareci, öğretmeni öğrenci ve çalışanları için farkındalık yaratmak.
- Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu davranışları online olarak modellemek ve teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme gereksiniminin farkında olmak.
- Okuldaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.

- Bu politikanın, yönetim organı, öğretmenler, destek personeli, harici yükleniciler, ziyaretçiler, gönüllüler ve okul adına hizmet veren veya bunları yerine getiren diğer kişiler (toplu olarak bu politikada ´personel´ olarak anılacaktır) dahil olmak üzere tüm personel için geçerlidir) yanı sıra çocuklar ve ebeveynleri kapsamasını sağlamak,

Sonuç olarak ana hedefimiz, internet erişimi ve kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarının kullanımı için bu güvenlik politikasının geçerli olmasıdır. Aynı zamanda öğrenciler, personel ya da diğer kişilere, çalıştıkları dizüstü bilgisayarlar, tabletler veya mobil cihazlar gibi uzaktan kullanım için okul tarafından verilen cihazlar için de geçerlidir.

TÜM ÇALIŞANLARIN KİLİT SORUMLULUKLARI ŞUNLARDIR:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Kabul Edilebilir Kullanım Politikalarını (AUP´lar) okumak ve onlara bağlı kalmak.
- Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
- Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında öğrencilerle nasıl ilişkili olabileceklerini bilmek.
- Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modellemeyi bilmek.
- Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirme.
- Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireylerin belirlenmesi ve uygun önlem alınmasını sağlamak.
- Olumlu öğrenme fırsatlarına vurgu yapmak.
- Bu alanda mesleki gelişim için kişisel sorumluluk almak.

GENÇLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Okulun kabul edilebilir kullanım politikalarını okumak ve onlara bağlı kalmak.
- Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
- Herhangi bir olumsuzlukla karşılaşılması durumunda, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.

Bireysel yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede:

- Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
- Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.
- Belli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.

EBEVEYNLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

- Okul Kabul Edilebilir Kullanım Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve mümkün olduğunca kendilerinin de bağlı kalmasını sağlamak.
- Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.
- Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.
- Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
- Okul veya diğer uygun kurumlardan, kendileri ve ya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.
- Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
- Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
- Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

C. ÇEVRİMİÇİ İLETİŞİM VE TEKNOLOJİNİN DAHA GÜVENLİ KULLANIMI

Okul / Web Sitesinin Yönetilmesi

- Web sitesinde iletişim bilgileri okul adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.
- Okul Müdürü yayımlanan çevrimiçi içerik için genel yayın sorumluluğunu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır.
- Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak üzere okulun yayın yönergelerine uyacaktır.
- Spam maillerden korunmak için e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayımlanacaktır.
- Öğrenci çalışmaları öğrencilerin izniyle ya da ebeveynlerinin izniyle yayımlanacaktır.
- Okul web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.
- Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

Çevrimiçi Görüntü Ve Videolar Yayınlama

- Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
- Okul , resimlerin ve videoların tümünün, veri güvenliği, Kabul Edilebilir Kullanım Politikaları, Davranış Kuralları, sosyal medya, kişisel cihazların ve cep telefonlarının kullanımı gibi diğer politikalar ve prosedürlere uygun şekilde yer almasını sağlayacaktır.

- Görüntü politikasına uygun olarak, öğrencilerin resimlerinin / videolarının elektronik olarak yayınlanmasından önce her zaman ebeveynlerin yazılı izni alınacaktır.

Video Konferans Kuralları

- Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin iznini isteyecektir.
- Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek.
- Velilerin rızası, öğrenciler video konferans faaliyetlerine katılmadan önce alınacaktır.
- Video konferans, sağlam bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir
- Sadece ana yöneticilere video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına erişim hakkı verilecektir.
- Eğitimsel video konferans servisleri için özel oturum açma ve şifre bilgileri yalnızca personellere verilecek ve gizli tutulacak.

Kişisel Cihazların ve Cep Telefonlarının Kullanımı

- Cep telefonlarının gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmalarını gerektirir .
- Gençlerin ve yetişkinlerin cep telefonlarının ve diğer kişisel cihazların kullanımı, okul tarafından kararlaştırılacak ve okul Kabul Edilebilir Kullanım veya Cep Telefonu Politikası dahil olmak üzere uygun politikalarda yer alacaktır.
- Şehit Serhat Sığınak Mesleki ve Teknik Anadolu Lisesi mobil teknolojilerle yapılan kişisel iletişimin, çocuklar, personel ve anne-babalar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak, bu tür teknolojilerin okulda güvenli ve uygun bir şekilde kullanılmasını gerektirir.

Öğrencilerin Kişisel Cihazlarını Ve Cep Telefonlarını Kullanımı

- Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
- Bilişim araçlarını, okul yönetimi ile öğretmenin bilgisi ve izni dışında konuşma yaparak, ses ve görüntü alarak, mesaj ve e-mail göndererek, bunları arkadaşlarıyla paylaşarak eğitim-öğretimi olumsuz yönde etkileyecek şekilde kullanmak aynı zamanda okul ders saatleri içerisinde telefon bulundurmak kesinlikle yasaktır.
- Öğrenciler ders başlamadan önce telefonlarını öğretmen masalarına koymakla yükümlüdür. Cep telefonunun amacı dışında kullanımı ihlali oluştuğunda, öğrenci, telefondaki özel verilerin korunmasını sağlamak amacıyla telefonunu kapatıp ders öğretmenine verir. Ders öğretmeni öğrenci telefonunu ilgili müdür yardımcısına teslim eder. Cep telefonu öğrenci velisine teslim edilinceye kadar güvenli bir yerde tutulur. Velisi dışında telefon kimseye teslim edilmez.
- Gençlerin cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir.

- Cep telefonları veya kişisel cihazlar, bir öğretmenin onayını alarak onaylanmış ve yönlendirilmiş müfredat tabanlı etkinlik kapsamında olmadıkları sürece dersler veya resmi okul saatlerinde öğrenciler tarafından kullanılamaz.
- Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleşecektir.
- Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul telefonunu kullanmasına izin verilecektir.
- Ebeveynlerin okul saatlerinde cep telefonuyla çocuklarıyla iletişim kurmamaları, okul idaresine başvurmaları önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir.
- Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vermelidirler.
- Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.
- Öğrencinin kişisel cihazında veya cep telefonunda bulunan materyalin yasadışı olabileceği veya cezai bir suçla ilgili kanıt sağlayabileceğinden şüpheleniliyorsa, cihaz daha ayrıntılı araştırma için polise teslim edilir.

Ziyaretçiler 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.
- Okul, ziyaretçilere kullanım beklentilerini bildirmek için uygun tabela ve bilgileri sağlayacak ve sunacaktır.
- Personelin uygun ve güvenli olduğunda sorunlara karşı çıkması beklenir ve her zaman ziyaretçilerin herhangi bir ihlalini idareye bildirecektir.

Gençlerin Katılımı Ve Eğitimi

- Öğrenciler arasında güvenli ve sorumlu internet kullanımının önemi ile ilgili farkındalık yaratmak için bir çevrimiçi güvenlik (e-Güvenlik) müfredatı oluşturulur ve okulun tamamında yer alır.
- Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır.
- Müfredat geliştirme ve uygulama da dahil olmak üzere okul çevrimiçi güvenlik politikaları ve uygulamaları yazarken ve geliştirirken öğrenci katkıları aranacaktır.
- Öğrenciler, Kabul Edilebilir Kullanım Politikasını, yaşlarına ve yeteneklerine uygun bir şekilde okumak ve anlamak için desteklenecektir.
- Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.

- Kabul Edilebilir Kullanım beklentileri ve Posterler, Internet erişimi olan tüm odalarda yayınlanacaktır.
- İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.
- Dışarıdan destek, okulların dahili çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.
- Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarında ödüllendirecektir.
- Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

Personelin Katılımı Ve Eğitimi

- Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.
- Personel, İnternet trafiğinin izlenebileceğini ve tek bir kullanıcıya kadar izlenebileceğinin farkında olacak. Okul sistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış gereklidir.
- Personelin tüm üyelerine, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) temelde çeşitli şekillerde sağlanacaktır.
- Çalışanların tüm üyeleri, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Olumsuz durumlarda kamusal, disiplin veya hukuki önlemler alınabilir.
- Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklar.
- Okul, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.

Ebeveynlerin Katılımı Ve Eğitimi

- Şehit Serhat Sığınak Mesleki ve Teknik Anadolu Lisesi, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.
- Ebeveynlerin dikkatleri, okul açıklamaları ve okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.
- Okulumuzun bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.
- Ebeveynler, Okula Kabul Edilebilir Kullanım Politikası´nı okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.
- Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.

- Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

Çevrimiçi Olaylara Ve Koruma Sorunlarına Yanıt Verme

- Okulun tüm üyeleri, sakıncalı mesajlaşma, çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.
- Okulun tüm üyeleri, filtreleme, sakıncalı mesajlaşma, siber zorbalık, yasadışı içerik ihlali vb. gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.
- Dijital Abone Hattı (DSL), daha sonra kaydedilecek olan çocuk koruma endişelerini içeren herhangi bir çevrimiçi güvenlik (e-Güvenlik) olayı hakkında bilgilendirilecektir.
- İnternet´in yanlış kullanımı ile ilgili şikayetler, okulun şikayet prosedürleri kapsamında ele alınacaktır.
- Çevrimiçi / siber zorbalık ile ilgili şikayetler, okulun zorbalık karşıtı politikası ve prosedürü kapsamında ele alınacaktır.
- Personelin yanlış kullanımı ile ilgili herhangi bir şikayet okul müdürüne yönlendirilecektir.
- Okul şikayet prosedürü öğrencilere, velilere ve personele bildirilecektir.
- Şikayet ve ihbar prosedürü personele bildirilecektir.
- Okulun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar.
- Okulun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatılacak ve okul camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatacaktır.
- Okul, çevrimiçi güvenlik (e-Güvenlik) olaylarını, uygun olduğunda, okul disiplini / davranış politikasına uygun olarak yönetir.
- Okul, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.
- Herhangi bir soruşturma tamamlandıktan sonra okul bilgi alacak, öğrenilen dersleri belirleyecek ve değişiklikleri gerektiği gibi uygulayacaktır.
- Sorunları çözmek için ebeveynlerin ve gençlerin okulla iş birliği içinde çalışması gerekir.

e-Safety POLICY

ŞEHİT SERHAT ŞİNAK VOCATIONAL AND TECHNICAL ANATOLIAN HIGH SCHOOL

e-Safety POLICY and OBJECTIVES

With changing and developing technological opportunities, it is an important issue to inform our students about how to overcome security problems and how to benefit from technology at a high level. For this reason, it is considered important for every school to have a School Security Policy. We are a school with a Safe Internet School Policy.

A. OUR E-SAFETY POLICY:

1. Our school has social networks such as its website and Instagram account. Data published on these networks is shared with administrator and editor control.

2. In our school, mobile phones are kept turned off during lessons, and teachers who do eTwinning projects use them when necessary for project work.

3. Seminars are regularly organized for classes by the guidance service on topics such as ICT addiction, correct and safe use of ICT, and Cyber Bullying.

4. There are fixed boards in our school regarding the correct and safe use of ICT.

5. There are warning and informative signs for all students in our school's ICT laboratories.

6. The teachers of our school have received distance and face-to-face training such as Cyber Bullying and the correct and safe use of ICT, given by the Ministry of National Education.

7. "Safer Internet Day" is celebrated in our school.

8. On our school's website, there is a link to https://www.guvenlicocuk.org.tr/ regarding e-security. Our school stakeholders can obtain information on the subject whenever they want.

9. Our guidance counselors and information technology teachers convey their knowledge to our students about internet ethics and safe internet use.

10. 21st century communication skills are important in our school. In this regard, studies are carried out to improve the ICT usage skills of our students.

11. In our school, activities are carried out to raise awareness among our stakeholders about being a digital citizen.

B. PURPOSE OF E-SAFETY POLICY IN OUR SCHOOL:

• To protect and ensure the security of all members of our school online.

• To raise awareness for the administrators, teachers, students and employees of Şehit Serhat Sığak Vocational and Technical Anatolian High School about the potential risks and benefits of technology.

• Ensuring all staff work safely and responsibly, modeling positive behavior online and being aware of the need to manage their own standards and practices when using technology.

• Clearly define procedures to be used when responding to online security concerns known to all members of the school.

• This policy applies to all staff, including the governing body, teachers, support staff, external contractors, visitors, volunteers and others who provide or perform services on behalf of the school (collectively referred to in this policy as 'staff') as well as ensuring that children and parents are included,

As a result, our main goal is that this security policy applies to the use of information communication devices, including internet access and personal devices. It also applies to devices issued to students, staff or others by the school for remote use, such as laptops, tablets or mobile devices on which they work.

THE KEY RESPONSIBILITIES OF ALL EMPLOYEES ARE:

• Contributing to the development of online security policies.

• Read and adhere to Acceptable Use Policies (AUPs).

• Being responsible for the security of school systems and data.

• Have an awareness of a range of different online security issues and how they may relate to students in their care.

• Knowing how to model good practices when using new and emerging technologies.

• Link online safety training to the curriculum wherever possible.

• Following school protection policies and procedures to identify individuals with concerns and ensure appropriate action is taken.

• Emphasizing positive learning opportunities.

• Taking personal responsibility for professional development in this field.

THE MAIN RESPONSIBILITIES OF YOUTH ARE:

• Contributing to the development of online security policies.

• Read and adhere to the school's acceptable use policies.

• Respecting the feelings and rights of others online and offline.

• If anything goes wrong, seek help from a trusted adult and support others facing online security issues.

At a level appropriate to their individual age, abilities and weaknesses:

• Taking responsibility for protecting themselves and others online.

• To be responsible for their own awareness and learning regarding the opportunities and risks brought by new and emerging technologies.

• Assess the personal risks of using a particular technology and act safely and responsibly to limit these risks.

PARENTS' MAIN RESPONSIBILITIES ARE:

• Read the School Acceptable Use Policies, encourage their children to adhere to this policy, and ensure that they do so themselves as much as possible.

• Discussing online safety issues with their children, supporting the school's online safety approaches, and reinforcing appropriate safe online behavior at home.

• Modeling safe and appropriate use of technology and social media.

• Identify changes in behavior that indicate the child is at risk of harm online.

• Seeking help or support from school or other appropriate agencies if they or their children encounter problems or problems online.

• Contributing to the creation of the school's online security policies.

• Using school systems, such as learning platforms and other network resources, in a safe and appropriate manner.

• To be responsible for their own awareness and learning regarding the opportunities and risks brought by new and emerging technologies.

C. SAFER USE OF ONLINE COMMUNICATION AND TECHNOLOGY

Managing the school / website

• Contact information on the website will be school address, email and phone number. Personal information of staff or students will not be published.

• The Head of School will take overall editorial responsibility for published online content and will ensure that the information is accurate and appropriate.

• The website will comply with the school's publishing guidelines, including accessibility, respect for intellectual property rights, privacy policies and copyright.

• Email addresses will be carefully published online to protect against spam.

• Student works will be published with the permission of the students or their parents.

• The administrator account of the school website will be protected by being encrypted with an appropriately strong password.

• The school will post information about safeguarding, including online safety, on the school website for members of the community.

Post images and videos online

• The school will ensure that all images and videos shared online are used in accordance with the school image use policy.

• The School will ensure that all images and videos are included in accordance with other policies and procedures such as data security, Acceptable Use Policies, Code of Conduct, social media, use of personal devices and mobile phones.

• In accordance with the image policy, written parental consent will always be obtained prior to electronic release of students' images/videos.

Video Conferencing Rules

• Students will ask for permission from a teacher before making or responding to a video conference call or message.

• Video conferencing will be moderated appropriately for the age and ability of the students.

• Parents' consent will be obtained before students participate in video conferencing activities.

• Video conferencing will take place through official and approved communication channels, following a sound risk assessment

• Only main administrators will be given access to video conference management areas or remote control pages.

• Special login and password information for educational video conferencing services will be given only to personnel and will be kept confidential.

Use of Personal Devices and Mobile Phones

• The widespread ownership of mobile phones and other personal devices among youth and adults requires all members to take steps to ensure responsible use of mobile phones and personal devices.

• The use of mobile phones and other personal devices by young people and adults will be determined by the school and will be included in appropriate policies, including the school Acceptable Use or Mobile Phone Policy.

• Şehit Serhat Sığak Vocational and Technical Anatolian High School is aware that personal communication through mobile technologies is an accepted part of daily life for children, staff and parents; however, it requires the safe and appropriate use of such technologies in school.

Students' use of personal devices and mobile phones

• Students will receive training on the safe and appropriate use of personal devices and mobile phones.

• It is strictly forbidden to use IT devices in a way that will negatively affect education by talking, taking audio and video, sending messages and e-mails, and sharing them with friends, without the knowledge and permission of the school administration and the teacher. At the same time, it is strictly forbidden to have a phone during school class hours.

• Students are obliged to place their phones on the teacher's desks before the lesson starts. When a violation of misuse of the mobile phone occurs, the student turns off his phone and gives it to the teacher in order to protect the private data on the phone. The course teacher delivers the student's phone to the relevant assistant principal. The mobile phone is kept in a safe place until it is handed over to the student's parent. The phone cannot be handed over to anyone except the parent.

• All use of young people's mobile phones and personal devices will be in accordance with the acceptable use policy.

• Cell phones or personal devices may not be used by students during lessons or official school hours unless they are part of an approved and directed curriculum-based activity with the approval of a teacher.

• Children's use of mobile phones or personal devices in educational activities will only take place when approved by the school administration.

• If a student feels the need to call their parents, they will be allowed to use the school phone.

• Parents are advised not to contact their children via mobile phone during school hours and to contact the school administration. Exceptions may be allowed in exceptional cases as approved by the teacher.

• Students should only give their phone numbers to trusted friends and family members.

• Students will be taught the safe and appropriate use of mobile phones and personal devices and will be aware of limits and consequences.

• If it is suspected that material found on a student's personal device or mobile phone may be illegal or may provide evidence of a criminal offence, the device will be handed over to the police for further investigation.

Visitors are prohibited from using personal devices and mobile phones.

• Parents and visitors must use mobile phones and personal devices in accordance with the school's acceptable use policy.

• Use of mobile phones or personal devices by visitors and parents to take photographs or videos must be in accordance with the school image use policy.

• The school will provide and provide appropriate signage and information to inform visitors of usage expectations.

• Staff are expected to address problems when appropriate and safe and will always report any infractions by visitors to management.

Youth Participation And Education

• An online safety (e-Safety) curriculum is created and included throughout the school to raise awareness among students about the importance of safe and responsible internet use.

• Training on safe and responsible use will be provided before internet access.

• Student input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.

• Students will be supported to read and understand the Acceptable Use Policy in a manner appropriate to their age and abilities.

• All users will be notified that their network and internet usage will be monitored.

• Acceptable Use expectations and Posters will be posted in all rooms with Internet access.

• Safe and responsible use of the internet and technology will be strengthened across the curriculum and across all subjects.

• External support will be used to complement and support schools' internal online safety (eSafety) training approaches.

• The school will reward students when they use technology in a positive way.

• The school will implement peer education to improve online security in accordance with students' needs.

Staff İnvolvement And Training

• Online security (eSafety) policy will be formally provided and discussed for the participation of all employees and will be reinforced and emphasized as part of our responsibility to protect.

• Staff will be aware that Internet traffic can be monitored and traced back to a single user. Discretion and professional conduct are required when using school systems and devices.

• All members of staff, professionally and personally, will be provided with a variety of up-to-date and appropriate staff training on safe and responsible Internet use on a regular (at least annual) basis.

• All members of staff will be aware that their online behavior may affect their role and reputation within the school. In adverse cases, public, disciplinary or legal measures may be taken.

• Members of staff with responsibility for managing filtering systems or monitoring ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.

• The school highlights useful online tools that staff should use according to students' ages and abilities.

Parent İnvolvement And Education

• Şehit Serhat Sığak Vocational and Technical Anatolian High School recognizes that parents have an important role to play in helping children become reliable and responsible users of the internet and digital technology.

• Parents' attention will be directed to the school online security (e-Safety) policy and expectations in school statements and on the school website.

• As part of our schooling, parents will be required to read online safety information.

• Parents will be encouraged to read the School's Acceptable Use Policy and discuss its implications with their children.

• Parental information and guidance on online safety will be available to parents in a variety of formats.

• Parents will be encouraged to role model positive behavior for their children online.

Responding To Online Incidents And Protection Issues

• All members of the school must refrain from objectionable texting, online/cyber bullying, etc. will be made aware of the range of online risks that may be encountered, including: This will be emphasized within staff training and educational approaches to students.

• All members of the school are responsible for filtering, objectionable messaging, cyber bullying, illegal content violations, etc. will be informed of the procedure for reporting online security (e-Safety) concerns, such as

• The Digital Subscriber Line (DSL) will be notified of any online safety (eSafety) incident involving child protection concerns which will then be recorded.

• Complaints regarding misuse of the Internet will be handled within the scope of the school's complaints procedures.

• Complaints regarding online/cyber bullying will be dealt with under the school's anti-bullying policy and procedure.

• Any complaints regarding staff misuse will be directed to the school principal.

• The school complaint procedure will be communicated to students, parents and staff.

• The complaint and notification procedure will be communicated to the personnel.

• All members of the school should be aware of the importance of confidentiality and the need to follow official school procedures for reporting concerns.

• All members of the school will be reminded of safe and appropriate behavior online and the importance of not posting any content, comments, images or videos that may cause harm, distress or offense to any other member of the school community.

• The school manages online security (eSafety) incidents in accordance with the school discipline/conduct policy, where appropriate.

• The school notifies parents of concerns when needed.

• Once any investigation is completed, the school will debrief, identify lessons learned, and implement changes as necessary.

• Parents and young people need to work collaboratively with the school to solve problems.