

## ASSESSMENT INFORMATION

Organisation	<a href="#">Sandıklı Zübeyde Hanım Mesleki ve Teknik Anadolu Lisesi</a>
Submitted by	<a href="#">Ayla Bahşi</a>
Submitted on	29.12.2020 @ 18:49:47
Uploaded files	
Survey PDF	<a href="#">Download</a>
Action plan PDF	<a href="#">Download</a>

## POINTS

### ASSESSMENT

Infrastructure score	14.0
Policy score	15.0
Practice score	14.0
Bonus score	0.0
Total score	43.0

Label





This school has been  
awarded with the  
**eSafety Label**

**Bronze**

valid until 06/2022

Action plan submitted by Ayla Bahşi for Sandıklı Zübeyde Hanım Mesleki ve Teknik Anadolu Lisesi - 28.09.2019 @ 23:53:49

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](http://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

- › 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.
- › 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](http://www.esafetylabel.eu/group/community/using-mobile-device-in-schools)).
- › It is good that in your school computer labs can easily be booked. Consider the option of integrating other digital devices into the lessons as using them provides best practise for pupils in dealing with new media. Ensure that safety issues are also discussed.

### Data protection

- › Having your learning and administration environments together can create a security risk. Ensuring security of staff's and pupils' private data is a fundamental role of the school. We recommend that your appointed eSafety manager/ICT coordinator, together with the staff and a technical expert, define and implement a strategy for separating learning and administration environments or ensuring the equivalent highest level of security between them. Read the fact sheet on Protecting sensitive data in schools at

[www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools](http://www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools).

- › 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 good practise that the member of staff responsible is fully aware of installed software and their license status.

## IT Management

- › In the interests of innovative pedagogical practice, it may seem necessary to allow staff and pupils to upload software to school-owned hardware, however this should only be done by the person in charge of the school ICT network in conformity with the School Policy. Staff and pupils should be aware of this through the Acceptable Use Policy they are required to sign. All new software uploaded to school equipment needs to be in conformity with licensing requirements.
- › It is good that staff members with questions about software issues can contact a school helpdesk. Consider whether you need to provide training and/or guidance to new software that is installed on school computers. This is important to ensure that school members will take advantage of new features, but also that they are aware of relevant security and data protection issues.

## Policy

### Acceptable Use Policy (AUP)

- › This is good teaching practice, but you need to consolidate it with a section dedicated to mobile phone usage in your School Policy and your Acceptable Use Policy. Consult all stakeholders to develop this; the fact sheets on Using mobile phones at school ([www.esafetylabel.eu/group/community/using-mobile-device-in-schools](http://www.esafetylabel.eu/group/community/using-mobile-device-in-schools)) and School Policy ([www.esafetylabel.eu/group/community/school-policy](http://www.esafetylabel.eu/group/community/school-policy)) will provide helpful information.

### Reporting and Incident-Handling

- › It's good that you have a clear School Policy on handling out-of-school eSafety incidents; is the number of these declining? Start a discussion thread in the community on what other preventative measures or awareness raising activities could be used in order to reduce the number of issues further. Don't forget to anonymously document incidents on the Incident handling form ([www.esafetylabel.eu/group/teacher/incident-handling](http://www.esafetylabel.eu/group/teacher/incident-handling)), as this enables schools to share and learn from each other's strategies.
- › It is good practice to log cyberbullying incidents that occur in your school centrally, as you are contributing to building a data base of successful incident handling practices from schools across Europe that you and others can use in future. Make sure that pupils sign up to anti-bullying guidelines in your Acceptable Use Policy.

### Staff policy

- › 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.

- › In your school user accounts are managed in a timely manner. This is important as it decreases the risk of misuse.
- › Ensure that all staff understand the school's regulations on use of personal mobile devices in the classroom; these should be clearly communicated in the School Policy. Monitor the effectiveness of the policy and ensure that it is adhered to. You can also advise your staff to read the fact sheet Using mobile phones at school ([www.esafetylabel.eu/group/community/using-mobile-device-in-schools](http://www.esafetylabel.eu/group/community/using-mobile-device-in-schools)).

## Pupil practice/behaviour

- › 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.
- › 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

- › 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](http://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 eSafety in the curriculum

- › 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 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](#).
- › 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.

- › Ensure that the eSafety curriculum keeps up with emerging issues by making full use of all available resources and ensure that it builds on prior learning, bearing in mind that pupils will need different messages depending on how they are using the technology.

## 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.esafetylevel.eu/group/community/pupils-use-of-online-technology-outside-school](http://www.esafetylevel.eu/group/community/pupils-use-of-online-technology-outside-school).
- › Use Safer Internet Day as a mechanism to get the whole school community involved with online safety. The information and resources available at [www.saferinternetday.org](http://www.saferinternetday.org) offer an ideal opportunity to promote peer advocacy activities.
- › Try to engage pupils in peer mentoring and provide them with opportunities to share their thoughts and understanding with their peers. Also check out the resource section of the eSafety Label portal to get further ideas and resources.

## Sources of support

- › All staff should have some responsibility for eSafety. School counsellors, nurses etc. are well placed to provide advice and guidance on these issues and should be invited to contribute to developing and regularly reviewing your School Policy. Consider whether it is appropriate to provide training for these staff.
- › Dobro je, da staršem nudite podporo v zvezi z e-varnostjo, ko si to želijo. Premislite, ali bi bilo dobro vse starše redno obveščati prek spletne strani ali prek povezav v šolskem e-glasilu. Morda imate lahko tudi roditeljski sestanek. Poglejte si smernice o informacijah za starše na [www.esafetylevel.eu/group/community/information-for-parents](http://www.esafetylevel.eu/group/community/information-for-parents), kjer boste našli gradiva, ki jih lahko posredujete staršem, in ideje, ki jih lahko uporabite na roditeljskih sestankih.

## 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?

**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.**



Assessment form submitted by Ayla Bahşi for Sandıklı Zübeyde Hanım Mesleki ve Teknik Anadolu Lisesi - 28.09.2019 @ 23:53:49

## Infrastructure

### Technical security

**Question:** Are filtering levels uniform across schools or do they depend on user profiles (teacher, pupil, admin staff, etc.) and their level of maturity/seniority?

- **Answer:** There is a basic level of filtering which blocks pornography, violent and illegal content.

**Question:** Are existing ICT services regularly reviewed, updated and removed if no longer in use?

- **Answer:** Yes, this is part of the job description of the ICT coordinator.

### Pupil and staff access to technology

**Question:** Are staff and pupils allowed to use their own equipment on the school WiFi network? How is this monitored?

- **Answer:** Staff and pupils are able to access the WiFi using their own personal devices. Use is governed by a robust Acceptable Use Policy, which is agreed and understood by all.

**Question:** Are mobile phones and other digital devices allowed in school?

- **Answer:** Some teachers allow mobile phones to be used in class as part of the class activity, due to the potential learning benefits mobile phones and digital devices can bring to the classroom.

**Question:** What is the pupil/computer access in your school?

- **Answer:** There are specific computer labs, which can be booked by the teacher and the teachers make good usage of this option.

### Data protection

**Question:** Do you have separated learning and administration environments in your school?

- **Answer:** No, they are on the same server.

**Question:** Do you consistently inform all school members about of the importance of protecting devices, especially portable ones?

- **Answer:** Yes, we provide training/manuals around issues like these.

### Software licensing

**Question:** How is the software and license status managed?

- **Answer:** It is part of responsibility of the IT responsible to be able to produce an overview of software and license status at any moment.



## IT Management

**Question:** Are teachers and pupils allowed to install software to computers that are school property?

> **Answer:** Yes.

**Question:** Once new software is installed, are teachers trained in its usage?

> **Answer:** Whenever staff members have a question about software they can contact the school helpdesk.

## Policy

### Acceptable Use Policy (AUP)

**Question:** Does the school have a policy on the use of mobile devices / mobile phones?

> **Answer:** We sometimes use mobile phones as a pedagogical tool, but don't have a specific policy on their use at school.

### Reporting and Incident-Handling

**Question:** Does the school take any responsibility for any online incidents that happen outside the school?

> **Answer:** Yes, and all staff, pupils and parents understand this.

**Question:** Are incidents of cyberbullying logged centrally?

> **Answer:** Yes, we log incidents and also record them via the eSafety Label incident handling form.

### Staff policy

**Question:** Is there a School Policy that states how staff should behave online?

> **Answer:** Yes.

**Question:** What happens to a teacher's account once s/he changes her/his role or leaves the school?

> **Answer:** The administrator is informed and immediately deactivates the teacher account or adjusts rights where possible.

**Question:** Are teachers permitted to use personal mobile devices in the classroom?

> **Answer:** Yes.

### Pupil practice/behaviour

**Question:** Does your school have a policy that states how pupils should communicate electronically at school?

> **Answer:** Yes, these are defined in the AUP and taught to pupils across the curriculum.

**Question:** Is there a school wide hierarchy of positive and negative consequences to address pupils' online behaviour?

> **Answer:** Yes and this is clearly understood by all and applied consistently throughout the school.

### School presence online

**Question:** Is it possible for pupils to take part in shaping the school online presence?

> **Answer:** Yes, pupils have the possibility to feedback on our online presence.

**Question:** Does your school policy contain a section on the taking and publishing of photographs of, and by, pupils, parents and staff?

> **Answer:** Yes, we have a comprehensive section on this in our School Policy.

## Practice

### Management of eSafety eSafety in the curriculum

**Question:** Are pupils taught about the risks of sexting?

> **Answer:** Sexting is not specifically mentioned but pupils are educated about the permanence of images and risks associated with the use of social media and digital images.

**Question:** Are legal consequences of online actions discussed with pupils? Topics would include terms and conditions, online payments, copyright.

> **Answer:** Yes, in all grades.

**Question:** Do you talk about online extremism/radicalisation/hate speech as part of your online safety curriculum?

> **Answer:** Yes, we have integrated discussion and education about these issues into our curriculum.

**Question:** Is the eSafety curriculum progressive?

> **Answer:** A little.

### Extra curricular activities

**Question:** Does the school provide eSafety support for pupils outside curriculum time?

> **Answer:** Yes, when asked.

**Question:** Does your school celebrate 'Safer Internet Day'?

> **Answer:** Yes, some staff and pupils celebrate 'SID'.

**Question:** Do pupils do peer mentoring about eSafety?

> **Answer:** No.

### Sources of support

**Question:** Are other school services involved in eSafety issues (e.g. counsellors, psychologists, school nurse)?

> **Answer:** No.

**Question:** Does the school provide eSafety support for parents?

> **Answer:** Yes, when asked.

### Staff training

**Question:** Are teachers trained on the topic of cyberbullying?

› **Answer:** Yes, every teacher.

# e-Güvenlik ile ilgili konular okulumuz 9. ve 10. Sınıf Müfredatlarında İşlenmektedir.

ZÜBEYDE HANIM MESLEKİ VE TEKNİK ANADOLU LİSESİ								
BİLİŞİM TEKNOLOJİLERİ ALANI <b>BİLİŞİM TEKNOLOJİLERİNİN TEMELLERİ</b> DERSİ 9D SINIFI								
2020-2021 EĞİTİM ÖĞRETİM YILI ÜNİTELENDİRİLMİŞ YILLIK DERS PLANI								
SÜRE			HEDEF VE DAVRANIŞLAR	KONULAR	ÖĞRENME-ÖĞRETME YÖNTEM VE TEKNİKLERİ	KULLANILAN EĞİTİM TEKNOLOJİLERİ, ARAÇ VE GEREÇLERİ	DEĞERLER EĞİTİMİ	DEĞERLENDİRME (Hedef ve Davranışlara Ulaşama Düzeyi)
AY	HAFTA	DERS SAATI						
<b>ÖĞRENME BİRİMİ 1-BİLİŞİM ETİĞİ</b>								
EYLÜL	25.09.2020	3	1.Bilişim teknolojilerini ve internet (genel ağ) ortamını kullanma ve yönetme sürecinde dikkat edilmesi gereken etik ilkeleri açıklar. 2. Bilgi güvenliğinin önemini açıklar..	1. BİLİŞİM ETİĞİ 1.1. ETİK VE BİLİŞİM ETİĞİ KAVRAMLARI 1.1.1. Etik ve Bilişim Etiği 1.1.2. Bilişim Temel Hak ve Özgürlükleri 1.1.3. Kod Yazımında Etik İlkeler 1.1.4. Sosyal Medya Etiği 1.1.5. İnternet Etiği 1.2. BİLGİ VE BİLGİ GÜVENLİĞİ	Anlatım-Uygulama Soru-Cevap Ölçme Değ.	Tahta kalem, Modüller, Bilgisayar	ADALET	

EKİM	2.10.2020	3	<p>3. Bilgi güvenliğine yönelik tehditleri açıklar.</p> <p>4. Kişisel bilgisayar ve ağ ortamında bilgi güvenliğini sağlamaya yönelik işlemleri yürütür.</p> <p>5. Fikri mülkiyet hakkını açıklar.</p>	<p>1.3. TEMEL GÜVENLİK PRENSİPLERİ</p> <p>1.3.1. Bilgisayar Açılış Güvenliği</p> <p>1.3.2. Parola Güvenliği Prensipleri</p> <p>1.3.3. İnternet Erişim Güvenliği</p> <p>1.3.4. E-Posta Güvenliği</p> <p>1.3.5. Sosyal Medyaya Erişim Güvenliği</p> <p>1.3.6. Dosya Erişim ve Paylaşım Güvenliği</p> <p>1.3.7. Zararlı Yazılımlardan Korunma Prensipleri</p> <p>1.4. FİKRÎ VE SINAİ MÜLKİYET</p> <p>1.4.1. Telif Hakkı 1.4.2. Marka 1.4.3. Patent</p> <p>1.4.4. Faydalı Model 1.4.5. Tasarım 1.4.6. Ticari Sır</p>	Anlatım-Uygulama Soru-Cevap Ölçme Değ.	Tahta kalem, Modüller, Bilgisayar		
------	-----------	---	---	--	--	-----------------------------------	--	--

**2020—2021 EĞİTİM—ÖĞRETİM YILI ZÜBEYDE HANIM MESLEKİ VE TEKNİK ANADOLU LİSESİ**  
**BİLİŞİM TEKNOLOJİLERİ ALANI PROGRAMLAMA TEMELLERİ DERSİ**  
**ÜNİTELENDİRİLMİŞ YILLIK DERS PLANI**

<b>EYLÜL</b>	<b>21-25.09.2020</b>	<b>4</b>	<p>1. Davranışın etik olup olmadığını tespit eder.</p> <p>2. Bilişim etiği kavramına uygun olmayan örneklerle ilgili görsel materyal hazırlar.</p> <p>1. Bilgi güvenliği unsurlarını belirtir.</p> <p>2. Bilgi güvenliği yönetimi standardını ayırt eder.</p> <p>1. Bilgisayara giriş güvenliği aşamalarını gerçekleştirir.</p> <p>2. Güvenli parola oluşturur.</p> <p>3. Güvenli hesap oluşturur.</p> <p>5. Dosya erişim ve paylaşım güvenliği sağlar.</p> <p>6. Sistem ve verileri sağlıklı bir şekilde yedekler.</p> <p>7. Kişisel mobil cihaz güvenliğini sağlar.</p> <p><b>Atatürk'ün Milli Eğitime verdiği önem 15 Temmuz Demokrasi ve Millî Birlik Günü ve Önemi</b></p>	<p><b>MODÜL : BİLİŞİM ETİĞİ VE BİLGİ GÜVENLİĞİ</b> <b>KONU : ETİK KAVRAMI – BİLGİ KAVRAMI</b> <b>MODÜL : BİLİŞİM ETİĞİ VE BİLGİ GÜVENLİĞİ</b> <b>KONU : TEMEL GÜVENLİK PRENSİPLERİ</b></p> <p>1. Etik kavramını açıklar.</p> <p>2. Etik ilkelerini sıralar.</p> <p>3. Bilişim etiği kavramını açıklar.</p> <p>4. Bilişimde temel etik sorunları açıklar.</p> <p>5. Bilişimde temel hak ve özgürlükleri açıklar.</p> <p>6. Kod yazımında etik kuralları açıklar</p> <p>7. Sosyal medya etiğini açıklar</p> <p>8. İnternet etiğini açıklar</p> <p>1. Bilgi kavramını açıklar.</p> <p>2. Bilgi güvenliği kavramını açıklar.</p> <p>3. Bilgi güvenliği unsurlarını açıklar.</p> <p>4. Bilgi güvenliği yönetimi sistemi prensiplerini açıklar.</p> <p>5. Bilgi güvenliği yönetim sistemi metodolojisini açıklar.</p> <p>1. Bilgisayara giriş güvenliği aşamalarını açıklar.</p> <p>2. Parola güvenliği aşamalarını açıklar.</p> <p>3. E posta güvenliği aşamalarını açıklar.</p> <p>4. İnternet erişim güvenliği aşamalarını açıklar.</p> <p>5. Sosyal medya güvenliği aşamalarını açıklar.</p> <p>6. Sosyal mühendislikten korunma yöntemlerini açıklar.</p> <p>7. Dosya erişim ve paylaşım güvenliği aşamalarını açıklar.</p> <p>8. Sistem ve verilerin yedeklenmesi aşamalarını açıklar.</p> <p>9. Zararlı yazılımlardan korunma aşamalarını açıklar.</p> <p>10. Mobil cihaz güvenlik aşamalarını açıklar.</p>	<p>Anlatma, Soru cevap gösterip yaptırma</p>	<p>Tahta kalem, Modüller, Bilgisayar</p>	

**2020—2021 EĞİTİM—ÖĞRETİM YILI ZÜBEYDE HANIM MESLEKİ VE TEKNİK ANADOLU LİSESİ**  
**BİLİŞİM TEKNOLOJİLERİ ALANI PROGRAMLAMA TEMELLERİ DERSİ**

**ÜNİTELENDİRİLMİŞ YILLIK DERS PLANI**

<b>EYLÜL-EKİM</b>	<b>28-31.09.2020</b> <b>01-02.10.2020</b>	<b>4</b>	<b>MODÜL : BİLİŞİM ETİĞİ VE BİLGİ GÜVENLİĞİ</b> <b>KONU : SİBER SUÇLAR VE İSTİSMAR</b> <b>MODÜL : KODLAMAYA HAZIRLIK</b> <b>KONU : KODLAMA ÖNCESİ HAZIRLIK</b>	Anlatma, Soru cevap gösterip yaptırma	Tahta kalem, Modüller, Bilgisayar	
			<p>1.Siber suç kavramını araştırır. 2. Siber suçları içeren görsel materyal hazırlar.</p> <p>1. Bilişim hukukunun temel kavramlarını ayırt eder. 2. Bilişim suçlarını içeren görsel materyal hazırlar.</p> <p>01. Sayı sistemleri arasında dönüşümler yapar. 02. Yazacağı programa uygun programlama dilini kullanır.</p> <p>1. Siber uzay kavramını açıklar. 2. Siber suç kavramını açıklar. 3. Siber suç çeşitlerini açıklar. 4. Siber suçun sosyal ve ekonomik yaşama etkisini listeler. 5. Siber suçların tarihçesini açıklar. 6. Siber istismar kavramını açıklar. 7. Türkiye'nin Siber Güvenlik organizasyon yapısını açıklar.</p> <p>1. Bilişim hukukunun temel kavramlarını açıklar. 2. Bilişim suçlarının Türk Hukuku düzenindeki yerini açıklar. 3. Bilişim suçlarının uluslararası hukuk düzenindeki yerini açıklar. 4. Etik ile hukuk arasındaki ilişkiyi açıklar.</p> <p>01. Bilgisayarın çalışma mantığını açıklar. 02. Bir yazılımda olması gereken temel özellikleri listeler. 03. Yazılım çeşitlerini açıklar. 04. Programlama dili çeşitlerini listeler.</p>			

Okulumuzda e-Güvenlik kapsamında öğrencilerimizin fotoğraflarının paylaşılması hususunda velilerinden gerekli izin belgeleri toplanmıştır

### SANDIKLI ZÜBEYDE HANIM MTAL MÜDÜRLÜĞÜ ÖĞRENCİ SOSYAL MEDYA VELİ İZİN BELGESİ

Milli Eğitim Bakanlığımız 2017/12 Sayılı Genelgesi uyarınca, okulunuz Sandıklı Zübeyde Hanım MTAL ..... sınıfında eğitim görmekte olan, velisi bulunduğum ..... isimli öğrencinin eğitim öğretim faaliyetleri kapsamında alınan ses, görüntü ve video kayıtlarının ve aynı zamanda hazırlamış olduğu eserlerin (hikâye, resim, fotoğraf, şiir, vb.) Milli Eğitim Bakanlığı'na bağlı kurum ve kuruluşlarca kullanılan kurumsal internet siteleri ve sosyal medya hesaplarında yayınlanmasına;

İzin Veriyorum.

İzin Vermiyorum.

Gereğini arz ederim.

Okul Resmi İnternet Sitesi : <http://sandikliktml.meb.k12.tr/>

Okul Resmi Facebook Hesabı: <https://www.facebook.com/groups/75128955879390/>

Okul Resmi Youtube Hesabı : [https://www.youtube.com/channel/UCzn7llpqOk\\_miTkyL-lhI4g](https://www.youtube.com/channel/UCzn7llpqOk_miTkyL-lhI4g)

Tarih :

Velinin Adı ve Soyadı :

Velisinin İmzası :




# OKULUMUZDA E-TWINNING KAPSAMINDA BELGE ALAN ÖĞRETMENLERİMİZ




## KATILIM BELGESİ

**Sayın Ayla BAHSİ**

eSafety Label Hakkında Her Şey kursunu başarıyla tamamlayarak bu sertifikayı almaya hak kazandınız

  
**M. Fatih DOĞER**  
eTwinning Türkiye  
Ulusal Destek Servisi Koordinatörü


  
**M. Hakan BÜÇÜK**  
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü  
Daire Başkanı




## KATILIM BELGESİ

Sayın Ayla BAHSI

İnternet Güvenliği ve eTwinning Etiği kursunu  
başarıyla tamamlayarak  
bu sertifikayı almaya hak kazandınız

  
M. Fatih DOĞER  
eTwinning Türkiye  
Ulusal Destek Servisi Koordinatörü

  
M. Hakan BÜÇÜK  
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü  
Daire Başkanı



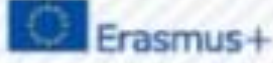
## KATILIM BELGESİ

Sayın AKİF ELDEM

İnternet Güvenliği ve eTwinning Etiği kursunu  
başarıyla tamamlayarak  
bu sertifikayı almaya hak kazandınız

M. Fatih DÖĞER  
eTwinning Türkiye  
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK  
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü  
Daire Başkanı



## KATILIM BELGESİ

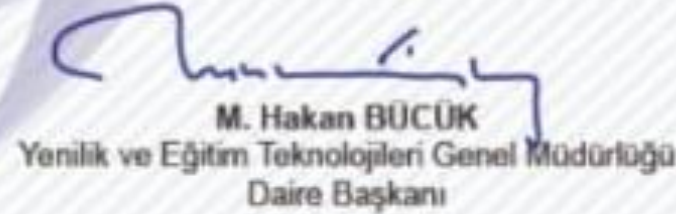
Sayın

AKİF ELDEM

Scratch ile Kodlama Eğitimi kursunu  
başarıyla tamamlayarak  
bu sertifikayı almaya hak kazandınız



M. Fatih DOĞER  
eTwinning Türkiye  
Ulusal Destek Servisi Koordinatörü



M. Hakan BÜCÜK  
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü  
Daire Başkanı

# ingilizce derslerimizde mufredat geregi e guvenlik konulari uzaktan egitime islenmektedir.

Dosya | F:/DOSYALAR/12%20kitaplar/12.%20sinif/12.Kitaplar/Kitaplar

**3** A. Discuss the positive and negative effects of cyber games and jot down some notes.

B. Watch the video and take notes about positive and negative effects of cyber games. Then, compare your notes with the notes based on the listening. Video 4.1

Positive Effects

Negative Effects

C. You will watch the same video again with some parts undubbed. These undubbed parts are for you to participate in the debate by using the statements below orally. Video 4.2

1. Do you mean they are useful?
2. I can't quite understand what you say.
3. You hit the nail on the head.
4. Some children try to move and act like superheroes and heroines and get seriously injured.
5. That doesn't seem to be a problem.
6. I don't see any point in playing such a game.

**4** A. The length of the lines in the below diagram shows the progress human beings made. How would you interpret the speed of change according to the diagram?

The progress human beings made



Participants (5)

- TA Teacher Ayla (Host, me)
- DG Damla G.
- S Selma
- S Sena
- V Vesile

Invite Mute All ...

Sena

Selma

Vesile

Damla G.

Aramak için buraya yazın

You are screen sharing. Stop Share

09:21  
31.12.2020

## THEME 4

COMING SOON

1 A. Do you think you are safe online?



B. Have you ever heard of or witnessed a cyber crime?

C. Read the text and answer the questions.

There is a Turkish saying which goes "There is no rose without a thorn" to emphasize that sometimes you have to take the bitter with the sweet. This is the same for the cyber world.

While enjoying the conveniences and advantages of cyber tools, you may be under serious threats. Since criminals have been where humans are, cyber world, in other words, the virtual world has turned out to be a new world for crimes. Just like the criminals in everyday life, cyber world has created its own criminals who are called hackers, cyber crooks. Their culprits are

Sena

Selma

Vesile

Damla G.

Participants (5)

TA Teacher Ayla (Host, me)

DG Damla G.

S Selma

S Sena

V Vesile

Invite

Mute All

You are screen sharing

Stop Share

09:21

11.12.2020