eSafety Label - Action Plan

Action plan submitted by Akgül Yıldırımer for Ilgın Atatürk Primary School - 25.01.2021 @ 18:57:27

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 good practice that your ICT services are regularly reviewed, updated and removed if no longer in use.

- 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

- All staff and pupils are allowed to use USB memory sticks in your school. This is good practice, and your Acceptable Use Policy should stipulate that all removable media is checked before use in the school systems. Check the fact sheet on Use of removable devices at www.esafetylabel.eu/group/community/use-of-removable-devices to make sure you cover all security aspects.

- 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.

Data protection

- 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.

- 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.

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.

- Your school has set a realistic budget for software needs. This is good. Ensure that it remains this way. You might also want to look into alternatives, e.g. Cloud services or open software.

IT Management

- There is a mechanism set up in your school that allows any staff member to make a request for new hard/software - a request that leads to an informed decision within a reasonable amount of time. This is great as this way teacher can benefit from new technologies while still staying inline with school policy.

- 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) Reporting and Incident-Handling

- Check that your School Policy includes all necessary information for teachers about handling issues when pupils knowingly or even inadvertently access illegal or offensive material online by going to the guidance set out by the teachtoday.de/en website (tinyurl.com/9j86v84). If such incidents arise in your school, make sure you anonymously fill out the eSafety Label Incident handling form (www.esafetylabel.eu/group/teacher/incident-handling) so that other schools can benefit from your experience.

- Please share the materials in which you tackle these issues especially with pupils and parents in the of the eSafety Label portal.

- 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), as this enables schools to share and learn from each other's strategies.

Staff policy

- 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.

- In your school user accounts are managed in a timely manner. This is important as it decreases the risk of

misuse.

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.

- When discussing eSafety pupils at your school can sometimes provide feedback on the activities . Involve them as much as possible so that the teacher recognises real life issues while the pupils are more engaged.

School presence online

- We recommend that you specifically nominate a web-experienced staff member to periodically check the school's online reputation. Monitoring such an important aspect on an ad hoc basis only is insufficient. Remember that this is the image that prospective parents will receive when they search for your school online.

- 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

- Technology develops rapidly. It is good practice that the member of staff responsible for ICT is regularly sent to trainings and/or conferences to be aware of new features and risks. Check out the Better Internet for Kids portal to stay up to date with the latest trends in the online world.

- It is good that all staff in your school are responsible for eSafety. However, it is good practice to appoint a person who will have overall responsibility for eSafety issues to provide the focus needed. Ideally this should be someone from the senior leadership team. Ensure that this person is involved in the development and regular review of your School Policy. She or he should not only be informed, but should also fill out the Incident handling form whenever an incident arises at www.esafetylabel.eu/group/teacher/incident-handling.

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

- 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 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.

Extra curricular activities Sources of support Staff training

- It should be a real benefit to your pupils that all staff receive regular training on eSafety issues. Continue to gather feedback from staff on the medium- and long-term benefits of the training and consult the eSafety Label portal to see suggestions for training courses at www.esafetylabel.eu/group/community/suggestions-for-online-training-courses.

- 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.

T.C.

MİLLÎ EĞİTİM BAKANLIĞI
KONYA-ILGIN ATATÜRK İLKOKULU

E-GÜVENLİK OKUL POLİTİKASI ve KURALLARI

AMAÇ:
- Politikamız,yöneticiler,öğretmenler,veliler,tümpersonelveöğrencileriçinhazırlanmışolup,interneterişimivebilgi iletişimcihazlarınınkullanımı içingeçerlidir.

- BodrumBilimveSanatMerkezi,e-güvenlikçalışmalarıileinternet,akıllıtahta,bilgisayar,dizüstübilgisayarveceptelefonlarınıkullanırken;öğrencilerin,velilerinveöğretmenlerinkorunmasınıamaçedinmiştir.

- İnternetinveteknolojininyaşamınönemlibirparçasıolmasısebebiyle,herkes,riskleriyönetmevestratejigeliştirmeyöntemlerinin öğrenilmesikonusunda bilinçlendirilmelidir.

SORUMLULUKLAR:
- Okuluveiçerisindekilerikorumakiçine-güvenlikkonusundasorumlulukalmak.
- Teknolojiyigüvenlivesorumlukullanmak.
- E-güvenlikpolitikalarınıngelişmesinekatkıdabulunmak.
- Olumluöğrenmeaşamasındameslekigelişimiçinsorumlulukalmak.
- Zarargörülmesidurumundatehlikeyigözlemleyipilgilibirimlereiletmek.

OKULWEBSİTESİ:
- Bodrum Bilim ve Sanat Merkezi olarak web sitemizde okulumuzun adres, telefon, fax ve e posta adres bilgileribulunmaktadır.
- Sitemizde yayınlanan tüm içerikler okul müdürümüzün onayından geçtikten sonra web sitesi komisyonu tarafındansiteyekonulmaktadır.
- Okulumuzunwebsitesiwebsitesikomisyonusorumluluğundaolupgüçlügüvenlikönlemlerialınmışdurumdadır.
- Öğrenciçalışmaları,velilerininizinleriyleyayınlanmaktadır.

GÖRÜNTÜVEVİDEOLARINPAYLAŞIMI
- Paylaşılan tüm öğrenci bazlı etkinliklerde,etkinliköncesindevelilerinizinlerialınmalıdır.
- Öğrencilertarafındanhazırlanacakolanbirvideohenüzhazırlanmadanönce,bununlailgiligörevalanöğrenciler,öğretmenlerindenizinalmalıdır.
- Videokonferans,resmiveonaylanmışsiteleraracılığıylayapılacaktır.

- Kullanıcılar,şahsisosyalmedyahesaplarında,okulöğrencileriveçalışanlarınınyeraldığıgörselleri,okulyetkilimercile ritarafından onaylanmadan paylaşamazlar.

KULLANICILAR:

- Öğrenciler tarafından hazırlanacak olan bir video henüz hazırlanmadan önce, bununla ilgili görev alan öğrenciler,öğretmenlerindenizinalmalıdır.
- Paylaşılantümöğrencibazlıetkinliklerde,etkinliköncesindevelilerinizinlerialınmalıdır.
- Videokonferans,resmiveonaylanmışsiteleraracılığıylayapılacaktır.
- Kullanıcılar,şahsisosyalmedyahesaplarında,okulöğrencileriveçalışanlarınınyeraldığıgörselleri,okulyetkilimercile ritarafından onaylanmadan paylaşamazlar.

İÇERİK:

- Videokonferansyapılırken,tümkullanıcılarınkatılabileceğisitelerüzerindenyapılacaktır.
- Videokonferansyapılmadanöncediğerokullarlailetişimkurulmuşolmasıgerekmektedir.
- Okul öğrenci ve çalışanlarını ilgilendiren/içinde bulunduran tüm içerik, ancak kontrol ve onay süreçlerindengeçtikten sonra, paylaşımaaçıkhale gelecektir.

İNTERNETİNVEBİLİŞİMCİHAZLARININ GÜVENLİKULLANIMI:

- Tüm okulumuza ait bilişim cihazlarımızı kullanım politikamıza uygun şekilde, gerekli filtrelemeleri yaparakgüvenlihale getirmiş durumdayız.
- Tüm çalışanlarımız, velilerimiz ve öğrencilerimiz etkili ve verimli çevrimiçi materyallerin kullanımı konusundabilgilendirilmiştir.
- İnternet; bilgiye ulaşmakta en önemli araçlardan biri haline gelmişken, bunu okuldaki müfredat ile ilişkilendirerekdoğrubilgiye engüvenli şekildeöğrencilerimiziveöğretmenlerimiziulaştırabiliyoruz.
- İnterneterişimlerimiziöğrencilerimizinyaşveyeteneklerinegöreentegreetmişdurumdayız.
- E-güvenlikvesiberzorbalıkkonularıbellideerslerimizinyıllıkplanlarınadahiledilmişolup,bukonulardayıliçindeöğrencilere bilgi aktarımıdevam etmektedir.
- Çevrimiçi materyaller öğretme ve öğrenmenin önemli bir parçası olup müfredat içinde aktif olarakkullanılmaktadır.
- Güvenliinternetgünüokulumuzdakutlanmaktadır.
- Okulumuzun akıllı tahtalarına kare kod uygulaması yüklenmiştir ve sadece öğretmenlerimizin telefonlarındakiuygulama ile açılabilmektedir. Öğrenciler akıllı tahtaya erişim için öğretmenlerinden veya okul idaresinden izinalmak zorundadır.

CEPTELEFONLARIVEKİŞİSELCİHAZLARINKULLANIMI:

- Okul içerisinde video ya da fotoğraf çeken öğrencilere yasalar ve Ödül ve Disiplin Yönetmeliği maddeleri gereğiişlemyapılmaktadır.
- Hertürlükişiselcihazlarınsorumluluğukişininkendisineaittir.
- Okulumuzbutürcihazlarınkullanımındandoğacakolumsuzsağlıkveyasalsorumluluklarıkabuletmez.
- Okulumuz kişisel cep telefonlarının ve bilişim cihazlarının kayıp, çalınma ve hasardan korunması için gerekli tümönlemlerialırfakat sorumluluk kişiye aittir.
- Okulumuz öğrencileri, velilerini aramaları gerektiği durumlarda okula ait olan telefonu bir okul idarecisigözetimindekullanabilirler.
- Öğrencilerimiz eğitim amaçlı (web 2 araçlarının kullanımı vb) kişisel cihazlarını kullanmak için okul yönetimindenizinalmalıdır.
- Velilerimiz okul saatleri içerisinde öğrencileriyle görüşme yapmamaları gerektiği konusunda bilgilendirilirler. Eğerzorunluhallervar iseokulyönetimindenizinalarak görüşmeyapmalarısağlanmalıdır.
- Öğrencilerimizceptelefonnumaralarınıyalnızcagüvenilirkişilerlepaylaşmaları,tanımadıklarıgüvenilirbul madıkları kişilerle cep telefonu gibi kişisel bilgilerini paylaşmamaları gerektiği konusundabilinçlendirilmektedirler.
- Çalışanlar (öğretmen, idareci, personel vb) kişisel cep telefonlarını ders saatlerinde sessize alarak ya da kapatarakgörevlerinedevametmelidir.
- Çalışanlar(öğretmen,idareci,personelvb)okulpolitikasınaaykırıdavranışlardabulunursadisiplinişlemleribaşlatı lır.
- Kurum çalışanları (öğretmen, idareci, personel vb) ve öğrenciler sosyal medya ya da sohbet programları üzerindenöğrenciya da kurumçalışanlarındangelecekolanya dakendilerinin göndereceklerihertürlüiçerikve

mesajlaşmanın hukuki sorumluluğunu taşımaktadır, uygunsuz olabilecek her türlü içerik ve mesajlaşma ivedilikleokulyönetimiilepaylaşılır.Böylebirdurumamahalvermemekiçingerekenönlemleralınır.

E-GÜVENLİKEĞİTİMİ:

- Öğrenciler için e-güvenlik müfredatı ilgili derslerin yıllık planlarına eklenerek öğrenciler bu konulardabilgilendirilir.
- Öğrencilerimizin ihtiyaçları doğrultusunda çevrim içi güvenliği geliştirmek için sınıf rehber öğretmenleri akraneğitimiuygulamaktadır.
- Teknolojiyiolumlukullananöğrencilerödüllendirilecektir.
- Çevrimiçigüvenlikpolitikasıtümçalışanlarımızaresmiolarakduyurulacaktır.
- Güvenli İnternet Günü okulumuzda kutlanmaktadır. Bu güne yönelik okul koridorları ve sınıflarda panoçalışmalarımızve sosyal medyapaylaşımlarımızolmaktadır.

ÇEVRİM İÇİOLAYLARVEKORUMA:

- Okulumuzuntümüyeleriçevrimiçirisklerkonusundabilgilendirilecektir.Eğitimleryapılıpiçerikleraçıklanacaktır.
- Okulumuzda yasadışı içerik, güvenlik ihlali, siber zorbalık, cinsel içerikli mesajlaşma, çocuk istismarı, kişisel bilgigüvenliğigibi konulardabilgilendirme çalışmaları yapılmaktadır.
- OkulumuzdaGüvenliInternetGünükutlanmaktadır.
- Okulumuzda internet, bilgi teknolojileri ve ekipmanlarının yanlış kullanımı ile ilgili tüm şikayetler okul müdürünebildirilecektir.
- Okulumuzun tüm üyeleri gizlilik ve güvenlik endişelerini ortadan kaldırmak için resmi okul kurallarına uygunşekildedavranmalarıhususunda bilgilendirilir.
- Yaşananolumsuzluklardaokulgerekliişlemleriyapmaklasorumludur.
- Sorunların çözümünde çalışanlar (öğretmen, idareci, personel vb), veliler ve öğrenciler okul ile birlikte hareketetmelidir.