**eSafety Label - Action Plan**

**Action plan submitted by Dilek Çelik for BARBAROS ORTAOKULU - 30.11.2020 @ 18:14:25**

**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.**

**Doldurulmuş Değerlendirme Formunuzu e-Güvenlik Etiketi portalına göndererek, okulunuzdaki e-Güvenlik durumunu analiz etme yolunda önemli bir adım attınız. Tebrikler! Okulunuzda e-Güvenliği daha da geliştirmek için neler yapabileceğinizi görmek için lütfen Eylem Planınızı dikkatlice okuyun. Eylem Planı, 3 temel alana bölünmüş yararlı tavsiyeler ve yorumlar sunar: altyapı, politika ve uygulama.**

# Infrastructure- Altyapı

## Technical security- Teknik güvenlik

Your school system is protected by a firewall but is sometimes bypassed for certain applications. While there may be some arguments for bypassing it, it is usually inadvisable to do so. If it is decided that the school policy will permit this, then it should only be implemented by an authorised technical manager and then on a restricted time basis.

Okul sisteminiz bir güvenlik duvarıyla korunmaktadır ancak bazen belirli uygulamalar için atlanır. Bunu atlamak için bazı argümanlar olsa da, genellikle bunu yapmak tavsiye edilmez. Okul politikasının buna izin vereceğine karar verilirse, o zaman sadece yetkili bir teknik müdür tarafından ve daha sonra sınırlı bir süre temelinde uygulanmalıdır.

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.

Her yaştan öğrencide bir eğitim yaklaşımı ve dayanıklılık oluşturmak da güvenli ve sorumlu çevrimiçi kullanımın anahtarıdır, bu nedenle tüm öğretmenleri öğrencileriyle iyi ve güvenli bir dijital vatandaş olma konusunda nasıl konuşacakları konusunda bir tartışma yapmak için bir araya getirin. Rol yapma ve grup oyunları aracılığıyla bu konu hakkında sınıfta gerçekleştirilebilecek tartışma örnekleri için www.europa.eu/youth/EU\_en adresini ziyaret edin.

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

ICT hizmetlerinizin düzenli olarak gözden geçirilmesi, güncellenmesi ve artık kullanılmıyorsa kaldırılması iyi bir uygulamadır.

## Pupil and staff access to technology Data protection Öğrenci ve personelin teknolojiye erişimi Veri koruma

Your new users are given a standard password and are asked to generate their own password on their first access. 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](https://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.

Yeni kullanıcılarınıza standart bir parola verilir ve ilk erişimlerinde kendi parolalarını oluşturmaları istenir. Parolalar, okul bilgi işlem sistemine benzersiz giriş noktaları sunar ve bazı temel parola güvenliği kuralları titizlikle uygulanmalıdır. Daha fazla bilgi için, www.esafetylabel.eu/group/community/safe-passwords adresindeki Güvenli şifreler hakkındaki bilgi formunu okuyun.

Bu kuralları Kabul Edilebilir Kullanıcı Sözleşmenize ekleyin ve yeni kullanıcılara standart bir "ilk erişim" şifresi vermekten kaçının.

There is a retention plan in place for your school detailing how specific school records are stored, archived and disposed. This is very good. Ensure that the plan is followed and review it regularly to ensure it relates to the Data Protection Act and other relevant legislation. Check the according fact sheet for more information.

Okulunuz için, belirli okul kayıtlarının nasıl saklandığını, arşivlendiğini ve imha edildiğini ayrıntılı olarak anlatan bir saklama planı vardır. Bu çok iyi. Planın izlendiğinden emin olun ve Veri Koruma Yasası ve diğer ilgili mevzuatla ilgili olmasını sağlamak için düzenli olarak gözden geçirin. Daha fazla bilgi için ilgili bilgi formunu kontrol edin.

Unprotected devices and even more so portable devices are a very high risk to data protection and not just to the device owner itself, but also to any person he has contact with. It is therefore crucial that all staff are informed and that this is also explained to pupils. Consider producing materials to share with all of your staff that raises awareness on this issue. This material should also be pointed out to new staff as part of there induction.

Korumasız cihazlar ve hatta daha fazlası taşınabilir cihazlar, veri koruma açısından çok yüksek risklidir ve yalnızca cihaz sahibinin kendisi için değil, aynı zamanda iletişim kurduğu herhangi bir kişi için de risklidir. Bu nedenle, tüm personelin bilgilendirilmesi ve bunun öğrencilere de açıklanması çok önemlidir. Bu konuda farkındalık yaratan tüm personelinizle paylaşmak için malzemeler üretmeyi düşünün. Bu materyal, oradaki indüksiyonun bir parçası olarak yeni personele de belirtilmelidir.

You have a good policy of keeping your learning and administration environments separate. It is good to ensure that staff training on managing these environments is up to date as you continue to review your policies. Share your policy with other eSafety Label users by uploading it to your school profile.

## Software licensing

Review the budget for software needs. You might also want to look into alternatives, e.g. Cloud services or open software.

You need to make sure that all the software in your school is legally licensed and that copies of the licences are held centrally. You also need to check with whoever supports your IT systems that the software will not compromise system security. Your school should develop a clear policy for software acquisition and it is good practice to centralise this process wherever possible.

## IT Management

It is good practise that your are training and/or providing guidance in the use of new software that is installed on school computers. This ensures that school members will take advantage of new features, but also that they are aware of security and data protection issues where relevant.

# Policy

## Acceptable Use Policy (AUP)

Regularly review the Mobile Phone Policy to ensure that it is fit for purpose and that it is being applied consistently across the school. The fact sheets on Using mobile phones at school ([www.esafetylabel.eu/group/community/using-mobile-device-in-schools](https://www.esafetylabel.eu/group/community/using-mobile-device-in-schools)) and School Policy ([www.esafetylabel.eu/group/community/school-polic](https://www.esafetylabel.eu/group/community/school-policy)y) will provide helpful information.

It is good that you have an Acceptable Use Policy (AUP) for pupils. You should now amend the AUP to include staff and the wider community. To ensure that your revised AUP is sufficiently comprehensive, take a look at the [fact sheet and check list on Acceptable Use Policy at www.esafetylabel.eu/group/community/acceptable-use](https://www.esafetylabel.eu/group/community/acceptable-use-policy-aup-)- [policy-aup-.](https://www.esafetylabel.eu/group/community/acceptable-use-policy-aup-)

## Reporting and Incident-Handling

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.

Online issues that take place outside of school will inevitably have an impact inside school. Consider whether the school needs to make a statement about how such issues will be dealt with in the School Policy and the Acceptable Use Policy. 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.

## Staff policy 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](http://www.esafetylabel.eu/group/teacher/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 are](http://www.esafetylabel.eu/group/teacher/my-school-area)a so that other schools can benefit from your experience.

## 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.

You have a dedicated person to monitor your school’s online reputation, and this is good practice. Always be aware of any new sites that may not be immediately apparent through a regular search. Keep up to date with the latest sites and monitor these periodically, as they can be particularly damaging for schools and their pupils and staff if they present a negative viewpoint.

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-schoo](https://www.esafetylabel.eu/group/community/taking-and-publishing-photos-and-videos-at-school)l) to see that your [School Policy covers all areas, then upload this section of your School Policy to your profile page via your M](http://www.esafetylabel.eu/group/teacher/my-school-area)y [school area so that other schools can learn from your good practice.](http://www.esafetylabel.eu/group/teacher/my-school-area)

Regularly check the content of the school's online presence on social media sites to ensure that there are no inappropriate comments. Set up a process for keeping the site/page up to date, and check the fact sheet on Schools on social networks ([www.esafetylabel.eu/group/community/schools-on-social-networks](https://www.esafetylabel.eu/group/community/schools-on-social-networks)) for further information to make sure that good practice guidelines have been followed. Get feedback from stakeholders about how useful the profile is.

# Practice

## Management of eSafety

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-polic](https://www.esafetylabel.eu/group/community/school-policy)y.

In your school, teachers are responsible for their own pupils’ online activity. There are many network security and user privacy, audit and procedural tool checks and balances that need to take place to ensure the safety of your pupils and the school networks, and these should be laid down in your School Policy. See our fact sheet on School Policy at [www.esafetylabel.eu/group/community/school-polic](https://www.esafetylabel.eu/group/community/school-policy)y.

To ensure this happens as efficiently and often as necessary, we advise that the Principal of your school appoints one individual staff member to look after eSafety management in the school. This person will be

responsible for seeing that all aspects included in your School Policy are discussed and looked at with other teachers as well as with pupils in the classroom.

To ensure that every staff member, pupil and parent is aware of her or his online rights and responsibilities, see the fact sheet on Acceptable Use Policy ([www.esafetylabel.eu/group/community/acceptable-use-policy-aup-](https://www.esafetylabel.eu/group/community/acceptable-use-policy-aup-)).

## eSafety in the curriculum

eSafety needs to be embedded across the whole curriculum regardless of whether this is a statutory obligation in your country. There are several very good schemes of work freely available which will support this; for further information see the fact sheet sheet Embedding eSafety in the curriculum at [www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum](https://www.esafetylabel.eu/group/community/embedding-online-safety-in-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 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.

## Extra curricular activities

Consider carrying out a simple survey in order to establish what pupils are doing when they go online. This will help to inform eSafety education within the school. Share your survey questionnaire and results in the eSafety Label community via your [My school area](http://www.esafetylabel.eu/group/teacher/my-school-area) (avoiding publishing any personal information) so that other schools can benefit from your work and even share their results with you for comparative purposes.

## Sources of support

Young people are more open to advice from their peers. Consider offering optional courses and/or school rewards on eSafety topics or similar that stimulate expert knowledge in pupils that then could become a point of reference for their peers.

## Staff training

In your school knowledge exchange between staff members is encouraged. This is beneficiary to the whole school. Upload PowerPoints, documents or similar of knowledge exchanges on eSafety topics via the uploading evidence tool, accessible also via the [My school are](http://www.esafetylabel.eu/group/teacher/resource-upload)a.

It is important that teachers are aware 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. Ensure that all teachers are provided with information of this. Have a look at the [Essie Survey of ICT in schools](http://essie.eun.org/).

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](http://www.esafetylabel.eu/group/teacher/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**](http://www.esafetylabel.eu/group/teacher/resource-upload) **on the** [**My school area**](http://www.esafetylabel.eu/group/teacher/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**](http://www.esafetylabel.eu/group/teacher/forum)**, and your** [**reporting of incidents**](http://www.esafetylabel.eu/group/teacher/incident-handling) **on the template provided are all also taken into account.**

© 2020 European Schoolnet