

# eSafety Label action plan for DÜZCE BORSA İSTANBUL MESLEKİ VE TEKNİK ANADOLU LİSESİ

# Infrastructure

## Technical security

* You urgently need to get virus protection for devices that need to be protected on the school network since only some of them are protected at the moment. Just one infected device can contaminate the school’s whole network and certain types of virus can even save illegal content to your server.

You should also include a paragraph on virus protection in both your school policy and your Acceptable Use Policy, and ensure that staff and pupils rigorously apply school guidelines. Check out the fact sheet on *Protecting your devices against malware* at [www.esafetylabel.eu/group/teacher/protecting-devices-against-malware](http://www.esafetylabel.eu/group/teacher/protecting-devices-against-malware).

* 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.

## 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/teacher/removable-devices](http://www.esafetylabel.eu/group/teacher/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

* 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.
* It is good that all users are attributed a different password by the system in your school. Remind all school members never to write their given password down anywhere, certainly not on a sticker on a computer! Also, ensure that the Acceptable Use Policy reminds staff and pupils to keep their passwords secure and not share them with others.

## 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.
* Ensure that all staff are aware of the procedure for purchasing new software and that all licenses are appropriate for the number of pupils and staff that will be using them. The [End-user license agreement](http://en.wikipedia.org/wiki/End-user_license_agreement) section in Wikipedia will provide useful information for understanding terms and conditions and comparing software agreements.

## IT Management

* It is good practice to ensure that the person in charge of the ICT network is fully informed of what software is on school-owned hardware and this should be clearly indicated in the School Policy and the Acceptable Use Policy. The person responsible for the network needs to be able to guarantee conformity with licensing requirements and that new software won’t interfere with network operation.
* In your school only the head master and/or IT responsible can acquire new software. Consider putting a system into place where teachers can ask for new software in a non-bureaucratic and timely fashion. This allows teachers to create a more engaging lesson without the temptation of unauthorized copying and its inherent dangers and costs.

# Policy

## Acceptable Use Policy (AUP)

* 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/teacher/acceptable-use-policy](http://www.esafetylabel.eu/group/teacher/acceptable-use-policy).
* It is excellent that eSafety is an integral part of several school policies. Do all staff make reference to it when appropriate through their teaching? Look for examples of good practice and share these with staff and pupils. Produce a short case study to highlight this good practice and upload it to your profile on the eSafety Label portal via your [My school area](http://www.esafetylabel.eu/group/teacher/my-school-area) as inspiration for other schools.

## Reporting and Incident-Handling

* Are all staff familiar with the procedure for dealing with material that could potentially be illegal? Is there a named person from the school senior leadership team who takes overall responsibility in this type of case? The procedure needs to be clearly communicated to all staff in the School Policy, and to staff and pupils in the Acceptable Use Policy. Remember to report and suspected illegal content to your national INHOPE hotline ([www.inhope.org](http://www.inhope.org/)).
* Ensure that all staff, including new members of staff, are aware of the guidelines concerning what to do if inappropriate or illegal material is discovered on a school machine. Ensure, too, that the policy is rigorously enforced. A member of the school's senior leadership team should monitor this.

## 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.
* It is good practice that the school policy includes information about risks with potentially non-secured devices, such as smartphones and that reference is made to it. Consider sharing your school policy via the uploading evidence tool, also accessible through the [My school area](http://www.esafetylabel.eu/group/teacher/resource-upload).

## 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](http://www.esafetylabel.eu/group/teacher/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](http://www.esafetylabel.eu/group/teacher/my-school-area) of the eSafety portal so that other schools can learn from it.

## School presence online

* Check the fact sheet on *Taking and publishing photos and videos at school* ( [www.esafetylabel.eu/group/teacher/photos-videos](http://www.esafetylabel.eu/group/teacher/photos-videos)) 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](http://www.esafetylabel.eu/group/teacher/my-school-area) so that other schools can learn from your good practice.
* Having an official school page on some of the more widely used/popular social networking sites can be useful for parents, pupils and the broader public if you use it to publicise your actions and events. However, exercise care when setting this up to ensure that someone from the school has control over posts etc. Check the fact sheet on *Schools on social networks* ([www.esafetylabel.eu/group/teacher/social-networks](http://www.esafetylabel.eu/group/teacher/social-networks)) for further information.

# Practice

## Management of eSafety

* In addition to a clear designation of responsibility to ensure that all necessary network security and user privacy checks are in place, it is essential that schools also have audit and procedural checks at regular intervals. Without this, a school will be leaving itself vulnerable. See our fact sheet on *School Policy* at [www.esafetylabel.eu/group/teacher/school-policy](http://www.esafetylabel.eu/group/teacher/school-policy) .

Although there should always be an overall lead person on eSafety just as you have in your school, everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties. Even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise problems. Use our fact sheet *Acceptable Use Policy* ([www.esafetylabel.eu/group/teacher/acceptable-use-policy](http://www.esafetylabel.eu/group/teacher/acceptable-use-policy)) to ensure that everyone plays their part in ensuring they are all the best and safest digital citizens they can be.

* Consider appointing a governor or board member who provides a liaison for eSafety issues. Consider also reporting on the number and type of eSafety incidents to the governing body on an annual basis when you also review your School Policy. See our fact sheet on *School Policy* [www.esafetylabel.eu/group/teacher/school-policy](http://www.esafetylabel.eu/group/teacher/school-policy).

## eSafety in the curriculum

* It is good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.
* It is very good that, in your school, pupils are taught from an early age on about responsibilities and consequences when using social media. Please share any resources through the uploading evidence tool, accessible also via the [My school area](http://www.esafetylabel.eu/group/teacher/resource-upload).

## Extra curricular activities

* Gather feedback from pupils to see what sort of additional eSafety support they would benefit from outside curriculum time. Could they be involved in delivering some of this to their peers? Check the resource section on the eSafety Label portal to find resources that will help them do this; check out the fact sheet on *Pupils' use of online technology outside school* at [www.esafetylabel.eu/group/teacher/social-media-pupils](http://www.esafetylabel.eu/group/teacher/social-media-pupils).
* How do you organise peer mentoring among pupils on eSafety? Check out the resources of the [ENABLE project](http://enable.eun.org/implementing_enable) and share your ideas in the [forum](http://www.esafetylabel.eu/group/teacher/forum) of the eSafety Label community so that other schools can benefit from your experience to establish a similar approach.

## Sources of support

* All staff should have some responsibility for eSafety. School counsellors, nurses, etc. are all well placed to provide advice and guidance on these issues and should be invited to contribute to developing and regularly reviewing your School Policy. Make the maximum use of their knowledge and skills and consider whether it is appropriate to provide training for them.
* Ask parents for feedback on the kind of eSafety support which is being provided for them and consider innovative ways to maximise the number of parents who are benefitting from, and accessing it. See the fact sheet *Information for parents* at [www.esafetylabel.eu/group/teacher/info-for-parents](http://www.esafetylabel.eu/group/teacher/info-for-parents) to find resources that could be circulated to parents and ideas for parent evenings.

## Staff training

* All staff need to be regularly updated about emerging trends in eSafety issues. Consider a needs-analysis to determine what different staff need from their training and consult the eSafety Label portal to see suggestions for training courses at [www.esafetylabel.eu/group/teacher/esafety-training-courses](http://www.esafetylabel.eu/group/teacher/esafety-training-courses).
* All teachers should be able to recognise signs of cyberbullying and be aware on how to best proceed. Make sure that your teachers are regularly trained bearing in mind the rapid changes of new technology. Also check the eSafety fact sheet on *Cyberbullying* at [www.esafetylabel.eu/group/teacher/cyberbullying](http://www.esafetylabel.eu/group/teacher/cyberbullying).