

Action plan submitted by sait AKAR for CUMHURİYET ANADOLU LİSESİ - 10.01.2020 @ 12:00:49

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

- › 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](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 very good that all your school devices are virus protected. Make sure you also have included 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. If you need further information, check out the fact sheet on Protecting your devices against malware at [www.esafetylabel.eu/group/community/protecting-your-devices-against-malware](http://www.esafetylabel.eu/group/community/protecting-your-devices-against-malware).

### 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](http://www.esafetylabel.eu/group/community/use-of-removable-devices) to make sure you cover all security aspects.

### 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 your email system is protected and that you have a policy for the transfer of pupil data in place. In this regard, it is important to draw up guidelines so that all staff are clear about what to do if they discover inappropriate or illegal content on school machines. For further information see the fact sheet on Protecting sensitive data ([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

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

## 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)

- › It is good that you have an Acceptable Use Policy for all members of the school community. Regularly review the AUP to ensure that it is still fit for purpose; to ensure that your 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-policy-aup-](http://www.esafetylabel.eu/group/community/acceptable-use-policy-aup-).
- › In your school policy issues are regularly discussed. This is good practice as it ensures staff and pupils are aware of them. Do pupils and staff also have to sign related documents to confirm their awareness?
- › It is good practise that whenever changes are put into place in your school, the school policies are revised if needed. Note though, that also changes outside the school can affect policies such as new legislations or changing technologies. Therefore please review your policies at least annually.

## Reporting and Incident-Handling

- › 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

- › 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](#).
- › There are dangers associated with the use of personal mobile devices in class. Consider why staff would need to use their device and, if appropriate, consider providing a school device. Advise staff to read the fact sheet on

Using mobile phones at school ([www.esafetylevel.eu/group/community/using-mobile-device-in-schools](http://www.esafetylevel.eu/group/community/using-mobile-device-in-schools)) and ensure that the guidelines to staff are clearly communicated in the School Policy.

## 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

- While your school has an online presence, pupils cannot take part in shaping it. Explore if there could be a way to involve pupils, maybe as part of a digital council. 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.
- It is important that a designated member of staff has an overview of any social networking profiles set up by representatives of your school. Check the fact sheet on Schools on social networks ([www.esafetylevel.eu/group/community/schools-on-social-networks](http://www.esafetylevel.eu/group/community/schools-on-social-networks)) for further information to make sure that good practice guidelines have been followed. Consider setting up a school social media profile to facilitate monitoring and showcase initiatives and achievements, as this can be a useful dissemination tool.

# 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.esafetylevel.eu/group/community/school-policy](http://www.esafetylevel.eu/group/community/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.esafetylevel.eu/group/community/acceptable-use-policy-aup-](http://www.esafetylevel.eu/group/community/acceptable-use-policy-aup-)) to ensure that everyone plays their part in ensuring they are all the best and safest digital citizens they can be.
- 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.esafetylevel.eu/group/community/school-policy](http://www.esafetylevel.eu/group/community/school-policy).

## eSafety in the 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 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 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

- › How do you organise peer mentoring among pupils on eSafety? Check out the resources of the [ENABLE project](#) and share your ideas in the [forum](#) of the eSafety Label community so that other schools can benefit from your experience to establish a similar approach.
- › Consider sharing the information you have about your pupils' online habits with other schools through the eSafety Label community. You could, for example, upload your latest survey findings on pupils' online habits to your school profile via your [My school area](#).

## Sources of support

- › It is great that in your school pupils are actively encouraged to become eSafety mentors. You might want to share your approach to strengthening this network with other teachers on the eSafety Label website via the forum or your school's profile page, so that others can replicate it.

## Staff training

- › 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](#).
- › 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.