

Action plan submitted by Hakan ÇANKAYA for Şehit Ahmet Hilmi Yiğit Mesleki ve Teknik Anadolu Lisesi - 19.01.2023 @ 13:54:44

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

- › Your school system is protected by a firewall. Ensure that the provision and management of the firewall are regularly reviewed and updated, as and when required.

### Pupil and staff access to technology 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.
- › It is good that your school records are stored in a safe environment, it is also necessary that they are archived and disposed with in line with the Data Protection Act. Ensure that a good records management system is put in place. Check the according fact sheet for more information.

### 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](#) section in Wikipedia

will provide useful information for understanding terms and conditions and comparing software agreements.

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

- › It is good practise that you 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 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](#) as inspiration for other schools.
- › 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.esafetymodel.eu/group/community/using-mobile-device-in-schools](http://www.esafetymodel.eu/group/community/using-mobile-device-in-schools)) and School Policy ([www.esafetymodel.eu/group/community/school-policy](http://www.esafetymodel.eu/group/community/school-policy)) will provide helpful information.
- › 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?

## 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](http://teachtoday.de/en) website ([tinyurl.com/9j86v84](https://tinyurl.com/9j86v84)). If such incidents arise in your school, make sure you anonymously fill out the eSafety Label Incident handling form ([www.esafetymodel.eu/group/teacher/incident-handling](http://www.esafetymodel.eu/group/teacher/incident-handling)) so that other schools can benefit from your experience.

## Staff policy

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

## Pupil practice/behaviour

- › 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.

- › 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.

## School presence 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](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.
- › 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](http://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.
- › 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.

## Practice

### Management of eSafety

- › It is good that the job description outlines that the member of staff responsible for ICT needs to keep up to date with new technologies. In addition, it would be good to regularly send the ICT responsible to trainings/conferences so (s)he can keep up with 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](http://www.esafetylabel.eu/group/teacher/incident-handling).

### eSafety in the curriculum

- › 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.
- › 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](#).

- › 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.
- › It is good to know that you are frequently using the online eSafety resources from your national Safer Internet Centre. Have you found these resources helpful in your school? Please send your feedback on their use and value to [info-insafe@eun.org](mailto:info-insafe@eun.org).

## 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.

## 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.esafetymal.eu/group/community/suggestions-for-online-training-courses](http://www.esafetymal.eu/group/community/suggestions-for-online-training-courses).

**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.**