

Action plan submitted by Nazife AYAZ for Alaeddin Keykubat Ortaokulu - 30.06.2020 @ 11:30:19

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

- It is good that in your school computer labs can easily be booked. Consider the option of integrating other digital devices into the lessons as using them provides best practise for pupils in dealing with new media. Ensure that safety issues are also discussed.
- You should organise a meeting with other teachers so you can discuss how the school could use social media and digital devices as an aid to learning in the classroom. Look at the outcomes and report from the SMILE project (Social Media in Learning and Education, <http://www.eun.org/teaching/smile>) to learn more about using social media in the classroom.
- 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

- 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.

## 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

- 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).

## Reporting and Incident-Handling

- 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](http://www.esafetylabel.eu/group/teacher/incident-handling)), as this enables schools to share and learn from each other's strategies.
- 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)).
- Please share the materials in which you tackle these issues especially with pupils and parents in the of the eSafety Label portal.

## Staff policy

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

- › 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](#).

## 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.

## 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.
- › 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.

# 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/community/school-policy](http://www.esafetylabel.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.esafetylabel.eu/group/community/acceptable-use-policy-aup](http://www.esafetylabel.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.
- › 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

- › It is commendable that you are able to provide an eSafety curriculum that keeps up with emerging issues. Continue to make use of new resources as they are made available. Can you upload to your school profile an outline of how you design the curriculum and links to some of the resources you use – this would be most helpful for other schools.
- › 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 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.
- › You may want to consider including sexting in your child protection policy to help to ensure a consistent whole-school approach to dealing with any incidents.

## Extra curricular activities Sources of support

- › It is good to know that other school services are involved in eSafety issues (e.g. counsellors, psychologists, school nurse). Are they also invited to contribute to developing and regular review of your School Policy? Publish a case study about how this is managed in your school on your school profile page on the eSafety Label project website, so that others can learn from your experience.

## 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](http://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?

**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.