

Action plan submitted by ŞENGÜL ATEŞ for CENGİZ TOPEL ANAOKULU - 18.01.2023 @ 19:11:51

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.
- › 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.

### Pupil and staff access to technology

- › 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.
- › 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.

### 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 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 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 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.esafetylevel.eu/group/community/acceptable-use-policy-aup](http://www.esafetylevel.eu/group/community/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.esafetylevel.eu/group/community/using-mobile-device-in-schools](http://www.esafetylevel.eu/group/community/using-mobile-device-in-schools)) and School Policy ([www.esafetylevel.eu/group/community/school-policy](http://www.esafetylevel.eu/group/community/school-policy)) will provide helpful information.
- › 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.
- › 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

- › 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)).

## Staff policy

- › As new technology and online practices emerge the borders of acceptable practice are constantly blurred. This

is something that needs to be discussed at staff meetings often. Could you create a tutorial on professional online conduct of staff and upload it to your school profile via your [My school area](#) so that other schools can benefit from your good practice?

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

## **Pupil practice/behaviour 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.
- › 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 eSafety in the curriculum**

- › While it is good that you discuss consequences of online actions terms and conditions, online payments and copyright with older pupils, consider discussing these also with young pupils.
- › It is good that eSafety is taught as part of the curriculum in your school. Ensure that all staff are delivering eSafety education where appropriate throughout the curriculum and not just through ICT or Personal Social and Health lessons. You/your staff may find some useful ideas and resources in the fact sheet Embedding eSafety in the curriculum at [www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum](http://www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum).
- › 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.
- › 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.

### **Extra curricular activities**

- › Try to engage pupils in peer mentoring and provide them with opportunities to share their thoughts and understanding with their peers. Also check out the resource section of the eSafety Label portal to get further

ideas and resources.

## 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.
- › 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.esafetylevel.eu/group/community/information-for-parents](http://www.esafetylevel.eu/group/community/information-for-parents) to find resources that could be circulated to parents and ideas for parent evenings.
- › It is great that you have a staff member which is knowledgeable in eSafety issues who acts as a teacher of confidence to pupils.

## 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 area](#).
- › 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.**