

Action plan submitted by Özlem KARASU for Zehra Ulusay Mesleki ve Teknik Anadolu Lisesi - 27.12.2020 @ 19:00:41

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 important that your ICT services are regularly reviewed, updated and removed if no longer in use. Installing the latest versions and patches often addresses security vulnerabilities without which your services might come under attack. Ensure that this is part of the job description of the ICT coordinator.

Pupil and staff access to technology

- › 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.
- › 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.

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.

- › Compliance with licensing agreements is important. Someone needs to have overall responsibility to ensure that this is happening and that all licenses are valid for purpose. The [End-user license agreement section](#) in Wikipedia will provide useful information for understanding terms and conditions and comparing software agreements.
- › It is good that you can produce an overview of installed software and their licences in a short time frame with the help of several people. Consider centralising this.

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.
- › There is a mechanism set up in your school that allows any staff member to make a request for new hardware/software - a request that leads to an informed decision within a reasonable amount of time. This is great as this way teachers can benefit from new technologies while still staying inline with school policy.

Policy

Acceptable Use Policy (AUP)

- › It is essential for all schools to have an Acceptable Use Policy (AUP) for staff and pupils. Consult with all stakeholders to draw up an AUP urgently. See the fact sheet and check list on Acceptable Use Policy at www.esafetylabel.eu/group/community/acceptable-use-policy-aup-
- › 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

- › 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).
- › Online issues that take place outside of school will inevitably have an impact inside school. Consider whether the school needs to make a statement about how such issues will be dealt with in the School Policy and the Acceptable Use Policy. Don't forget to anonymously document incidents on the Incident handling form (www.esafetylabel.eu/group/teacher/incident-handling), as this enables schools to share and learn from each other's strategies.
- › 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

- › Ensure that all staff, including new members of staff, are aware of the policy concerning online conduct. This should be a topic that is regularly discussed at staff meetings and clearly communicated in the School Policy, and to staff and pupils in the Acceptable Use Policy. Regularly review and update both documents as necessary.
- › In your school user accounts are managed in a timely manner. This is important as it decreases the risk of misuse.

Pupil practice/behaviour

- › It is good that pupils have the possibility to shape school activities when discussing eSafety, be it extra-curricular and curricular ones, based on what is going on in their daily lives. This way they will be more engaged and it also allows the teacher to recognise real life issues.

School presence online

- › 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) for further information to make sure that good practice guidelines have been followed. Get feedback from stakeholders about how useful the profile is.
- › You have a dedicated person to monitor your school's online reputation, and this is good practice. Always be aware of any new sites that may not be immediately apparent through a regular search. Keep up to date with the latest sites and monitor these periodically, as they can be particularly damaging for schools and their pupils and staff if they present a negative viewpoint.

Practice

Management of eSafety

- › In your school, teachers are responsible for their own pupils' online activity. There are many network security and user privacy, audit and procedural tool checks and balances that need to take place to ensure the safety of your pupils and the school networks, and these should be laid down in your School Policy. See our fact sheet on School Policy at www.esafetylabel.eu/group/community/school-policy.

To ensure this happens as efficiently and often as necessary, we advise that the Principal of your school appoints one individual staff member to look after eSafety management in the school. This person will be responsible for seeing that all aspects included in your School Policy are discussed and looked at with other teachers as well as with pupils in the classroom.

To ensure that every staff member, pupil and parent is aware of her or his online rights and responsibilities, see the fact sheet on Acceptable Use Policy (www.esafetylabel.eu/group/community/acceptable-use-policy-aup-).

- › It is good that you have a designated member of staff responsible for eSafety. Consider whether it would be helpful to have an eSafety committee comprising members from all groups of stakeholders. 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.

eSafety in the curriculum

- › 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](#).
- › It is good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.
- › It is good that sexting has been integrated into wider online safety education across the school. Are you able to assess the impact of this education? Does it help pupils to modify their behaviours? How do you know?
- › 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](#).

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/community/pupils-use-of-online-technology-outside-school.
- › 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.

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 is important that teachers are aware 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. Ensure that all teachers are provided with information of this. Have a look at the [Essie Survey of ICT in schools](#).

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.