

Action plan submitted by ebru ikbal uçar for Gediz 1 Eylül İmam Hatip Ortaokulu - 18.01.2023 @ 10:43:23

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

- › 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 for examples of discussions that can take place in the classroom on this topic, through role-play and group games.
- › 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

- › Ensure that the policy on mobile phones is being applied consistently throughout the school. Take a look at the fact sheet on Using Mobile Phones at School (www.esafetylevel.eu/group/community/using-mobile-device-in-schools).

Data protection

- › Your new users are given a standard password and are asked to generate their own password on their first access. Passwords offer unique entry points into the school computing system and some basic rules of password security should be rigorously applied. For further information, read the fact sheet on Safe passwords at www.esafetylevel.eu/group/community/safe-passwords.
Include these rules in your Acceptable User Agreement and avoid giving new users a standard "first access" password.
- › 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.
- › 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

- › 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 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.
- › 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 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 good that school policies are reviewed annually in your school. Ensure that they are also updated when changes are put into place that could affect them. All staff should be aware of the contents of the policy.
- › 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

- › 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), as this enables schools to share and learn from each other's strategies.
- › 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 website (tinyurl.com/9j86v84). If such incidents arise in your school, make sure you anonymously fill out the eSafety Label Incident handling form (www.esafetylabel.eu/group/teacher/incident-handling) so that other schools can benefit from your experience.

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.

- › 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

- › 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.
- › 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.
- › 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.esafetymail.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.

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.esafetymail.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.esafetymail.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.esafetymail.eu/group/teacher/incident-handling.

- › Technology develops rapidly. It is good practice that the member of staff responsible for ICT is regularly sent to trainings and/or conferences to be aware of 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.

eSafety in the curriculum

- › It is good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.
- › 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 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.esafetylevel.eu/group/community/embedding-online-safety-in-curriculum.

Extra curricular activities Sources of support

- › It is great that you have a staff member which is knowledgeable in eSafety issues who acts as a teacher of confidence to pupils.
- › 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.esafetylevel.eu/group/community/suggestions-for-online-training-courses.
- › 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](#).

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.

