

Action plan submitted by firdevs koç sağılr for MELİKŞAH ANADOLU LİSESİ - 25.01.2021 @ 12:07:51

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

- › 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.
- › Your school system is protected by a firewall but is sometimes bypassed for certain applications. While there may be some arguments for bypassing it, it is usually inadvisable to do so. If it is decided that the school policy will permit this, then it should only be implemented by an authorised technical manager and then on a restricted time basis.

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.
- › It is great that in your school laptops/tablets are easily accessible within a lesson. Using them provides best practise for pupils in dealing with new media. Ensure that safety issues are also discussed.

Data protection

- › It is good that all users are attributed a different password by the system in your school. Remind all school members never to write their given password down anywhere, certainly not on a sticker on a computer! Also, ensure that the Acceptable Use Policy reminds staff and pupils to keep their passwords secure and not share them with others.
- › 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.

- › 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

- › 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.

IT Management

- › In your school only the head master and/or IT responsible can acquire new software. Consider putting a system into place where teachers can ask for new software in a non-bureaucratic and timely fashion. This allows teachers to create a more engaging lesson without the temptation of unauthorized copying and its inherent dangers and costs.

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.
- › 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?
- › 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-.

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).
- › It is good practice to log cyberbullying incidents that occur in your school centrally, as you are contributing to building a data base of successful incident handling practices from schools across Europe that you and others

can use in future. Make sure that pupils sign up to anti-bullying guidelines in your Acceptable Use Policy.

Staff policy

- › 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](#).
- › 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.
- › 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.
- › 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

Practice

Management of eSafety

- › 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.esafetylevel.eu/group/teacher/incident-handling.

eSafety in the 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.
- › 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 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?

Extra curricular activities

- › It is good that you provide eSafety support for your pupils outside curriculum time when asked. Consider offering all pupils support to deal with online safety issues. It may be helpful to provide a "surgery" to help pupils to set their Facebook privacy etc. The eSafety Label portal provides resources that will be useful for this; check out the fact sheet on Pupils' use of online technology outside school at www.esafetymodel.eu/group/community/pupils-use-of-online-technology-outside-school.

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.
- › It is great that you have a staff member which is knowledgeable in eSafety issues who acts as a teacher of confidence to pupils.
- › It is good that there is an informal network of 'eSafety expert' pupils in your school. Explore ways to strengthen this, maybe through optional courses and/or school rewards on eSafety topics or similar.

Staff training

- › It is good practise that you provide information to teachers 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. You might want to have a look at the [Essie Survey of ICT in schools](#).
- › 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.

