

Action plan submitted by Ayşe Betül ESER for Kamile Gürkan Ortaokulu - 17.01.2023 @ 11:00:47

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.esafetymalware.com.
- › 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

- › 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.
- › 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.esafetymalware.com).

Data protection

- › It is good that your email system is protected and that you have a policy for the transfer of pupil data in place. In this regard, it is important to draw up guidelines so that all staff are clear about what to do if they discover inappropriate or illegal content on school machines. For further information see the fact sheet on Protecting sensitive data (www.esafetymalware.com).
- › 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 Management

- › 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 teacher can benefit from new technologies while still staying inline with school policy.

Policy

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.
- › 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.

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).

Staff policy

- › 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.
- › 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?

Pupil practice/behaviour

- › 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

- › 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.
- › 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.
- › 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.

Practice

Management of eSafety

- › Ensure that the governor or board member appointed for eSafety has the opportunity to receive regular training and also to ensure that colleagues are aware of eSafety issues. Involve your governing body in the development and regular review of your School Policy. See our fact sheet on School Policy www.esafetylabel.eu/group/community/school-policy.

eSafety in the curriculum

- › 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 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 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 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.
- › It is good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.

Extra curricular activities

- › Consider sharing the information you have about your pupils' online habits with other schools through the eSafety Label community. You could, for example, upload your latest survey findings on pupils' online habits to your school profile via your [My school area](#).

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.
- › 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.

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.

