

Action plan submitted by SEVDA BAYDAR for MUSTAFA ÇUKUR ORTAOKULU - 05.05.2022 @ 19:25:51

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

- › 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.
- › You urgently need to get virus protection for devices that need to be protected on the school network since only some of them are protected at the moment. Just one infected device can contaminate the school's whole network and certain types of virus can even save illegal content to your server. You should also include 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. Check out the fact sheet on Protecting your devices against malware at www.esafetylabel.eu/group/community/protecting-your-devices-against-malware.

Pupil and staff access to technology

- › All staff and pupils are allowed to use USB memory sticks in your school. This is good practice, and your Acceptable Use Policy should stipulate that all removable media is checked before use in the school systems. Check the fact sheet on Use of removable devices at www.esafetylabel.eu/group/community/use-of-removable-devices to make sure you cover all security aspects.
- › 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.
- › 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 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.esafetymail.eu/group/community/protecting-sensitive-data-in-schools).

Software licensing

- › 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. Staff should be briefed on who is the person responsible.
The [End-user license agreement](#) section in Wikipedia will provide useful information for understanding terms and conditions and comparing software agreements.

IT Management

- › It is good practice to ensure that the person in charge of the ICT network is fully informed of what software is on school-owned hardware and this should be clearly indicated in the School Policy and the Acceptable Use Policy. The person responsible for the network needs to be able to guarantee conformity with licensing requirements and that new software won't interfere with network operation.

Policy

Acceptable Use Policy (AUP)

- › When other school policies are reviewed, consider whether it would be appropriate to make references to eSafety, bearing in mind the wide range of issues that eSafety covers.
- › 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.esafetymail.eu/group/community/acceptable-use-policy-aup.
- › This is good teaching practice, but you need to consolidate it with a section dedicated to mobile phone usage in your School Policy and your Acceptable Use Policy. Consult all stakeholders to develop this; the fact sheets on Using mobile phones at school (www.esafetymail.eu/group/community/using-mobile-device-in-schools) and School Policy (www.esafetymail.eu/group/community/school-policy) will provide helpful information.

- › 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.

Reporting and Incident-Handling

- › It is a pity not to share the details and solutions applied to bullying incidents both with the staff members and via the eSafety Label incident handling form. Only in this way can you learn through experience and the successful incident handling practices of others. You should also make sure that anti-bullying guidelines are given to pupils and staff in your Acceptable Use Policy.
- › It is important to have a school-wide policy on handling issues when pupils knowingly or even inadvertently access illegal or offensive material online, since standards and practices can vary considerably from one teacher to the next. Guidance on this topic is provided on 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.esafetymail.eu/group/teacher/incident-handling) so that other schools can benefit from your experience.
- › 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.esafetymail.eu/group/teacher/incident-handling), as this enables schools to share and learn from each other's strategies.
- › (Cyber)bullying can be a serious problem and a whole-school approach should be taken to tackle it with a zero tolerance strategy. Read more about it in the eSafety fact sheet area.

Staff policy

- › In order to decrease the risks of misuse of user accounts, ensure that you put a procedure in place that immediately informs the ICT responsible to adjust user rights and/or deactivate them if the role of staff or pupil has changed.

Pupil practice/behaviour

- › Electronic communication guidelines for pupils should be clearly communicated in the Acceptable Use Policy. Communication between pupils can rapidly degenerate if school-wide standards are not set, giving rise to incidents such as cyberbullying. Learning about effective, responsible communication should also be part of the school curriculum, as it is a necessary competence for every young person. Discuss this at a staff meeting in order to define the standards you want to implement.

School presence online

Practice

Management of eSafety

- › It is good that the job description outlines that the member of staff responsible for ICT needs to keep up to date

with new technologies. In addition, it would be good to regularly send the ICT responsible to trainings/conferences so (s)he can keep up with 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

- › 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
- › It is good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.
- › Although these are sensitive issues, it is good to be proactive about raising awareness of them. Consider integrating some education around these issues into the overall eSafety curriculum.

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](#).
- › Try to develop further the engagement of pupils in peer mentoring and provide them with more 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 great that in your school pupils are actively encouraged to become eSafety mentors. You might want to share your approach to strengthening this network with other teachers on the eSafety Label website via the forum or your school's profile page, so that others can replicate it.
- › All staff should have some responsibility for eSafety. School counsellors, nurses etc. are well placed to provide advice and guidance on these issues and should be invited to contribute to developing and regularly reviewing your School Policy. Consider whether it is appropriate to provide training for these staff.

Staff training

- › All staff need to be regularly updated about emerging trends in eSafety issues. Consider a needs-analysis to determine what different staff need from their training and consult the eSafety Label portal to see suggestions for training courses at www.esafetymlabel.eu/group/community/suggestions-for-online-training-courses.
- › All teachers should be able to recognise signs of cyberbullying and be aware on how to best proceed. Make sure that your teachers are regularly trained bearing in mind the rapid changes of new technology. Also check the eSafety fact sheet on Cyberbullying at www.esafetymlabel.eu/group/community/cyberbullying.

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.