

Action plan submitted by Sümeyra GÜLMÜŞ for Reşat Benli İlkokulu - 02.01.2023 @ 19:49:33

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 good practice that your ICT services are regularly reviewed, updated and removed if no longer in use.

Pupil and staff access to technology

- › To have a policy that does not allow staff and pupils to use USB sticks is sensible and cautious but sometimes there are instances when use of USBs/removable media might be acceptable. To ensure that secure systems are maintained to the highest standards, include in your Acceptable Use Policy some information on use of removable storage devices. 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.
- › There are clear advantages for staff and pupils to bring their personal devices to school and to access internet on them. Besides supplementing the technical equipment available at school, this provides an important link between learning at home and at school and an opportunity to guide young people in responsible use. However, staff and pupil use of their own equipment on the school network needs to be addressed in an Acceptable Use Policy so that users are clear about which networks they should use and why. The Acceptable Use Policy needs to include clear guidance about which activities are permitted while on the school network, and what is not allowed.

Data protection

- › 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.
- › 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.

Software licensing

- › It is good practise that the member of staff responsible is fully aware of installed software and their license status.
- › 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.
- › 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.

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 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-.
- › Regularly review the Mobile Phone Policy to ensure that it is fit for purpose and that it is being applied consistently across the school. The fact sheets on Using mobile phones at school (www.esafetylevel.eu/group/community/using-mobile-device-in-schools) and School Policy (www.esafetylevel.eu/group/community/school-policy) will provide helpful information.

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).
- › Your teachers know how to recognise and handle (cyber)bullying. Think about ways to raise awareness also among pupils and parents. Check out the eSafety fact sheet for more information.

Staff policy

- › 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?
- › 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](#).

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.

School presence online

- › 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.
- › Check the fact sheet on Taking and publishing photos and videos at school (www.esafetylevel.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.
- › 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

- › 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.
- › 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.
- › 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.esafetymlabel.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.esafetymlabel.eu/group/community/acceptable-use-policy-aup-).

eSafety in the curriculum

- 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.esafetymlabel.eu/group/community/embedding-online-safety-in-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.

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.esafetymlabel.eu/group/community/pupils-use-of-online-technology-outside-school.
- 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](#).
- How do you organise peer mentoring among pupils on eSafety? Check out the resources of the [ENABLE project](#) and share your ideas in the [forum](#) of the eSafety Label community so that other schools can benefit from your experience to establish a similar approach.

Sources of support Staff training

- 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?
 - 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](#).
-

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.