

Action plan submitted by Burcu Kiper for Seydişehir Özel Eğitim Uygulama okulu - 27.11.2020 @ 17:39:17

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. Ensure that the provision and management of the firewall are regularly reviewed and updated, as and when required.

Pupil and staff access to technology

- › It is good that in your school computer labs can easily be booked. Consider the option of integrating other digital devices into the lessons as using them provides best practise for pupils in dealing with new media. Ensure that safety issues are also discussed.

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.esafetylabel.eu/group/community/safe-passwords.

Include these rules in your Acceptable User Agreement and avoid giving new users a standard "first access" password.

- › You have a good policy of encrypting pupil data and storing it safely. Ensure all new staff made aware of the procedures for encryption and data handling and that there is a named point of contact acting as the data controller for your school. Upload to your school profile some guidelines about protecting sensitive data through an encryption system so that other schools can benefit from your experience.

Software licensing

- › It is good practise that the member of staff responsible is fully aware of installed software and their license status.
- › Review the budget for software needs. You might also want to look into alternatives, e.g. Cloud services or open software.
- › 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 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.
- › 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 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.esafetylabel.eu/group/community/acceptable-use-policy-aup-.

Reporting and Incident-Handling

- › Have teachers received training on dealing with potentially illegal material? Is the procedure clearly indicated in the School Policy and the Acceptable Use Policy which all teachers and pupils have signed? All staff and pupils should be aware that they should report any suspected illegal content to the national INHOPE hotline (www.inhope.org).
- › 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.

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.

- › 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.
- › 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 partly has a school wide approach of positive and negative consequences for pupil behaviour. This is a good start, make sure that the policy and associated hierarchy applies to all on- and offline issues and is shared widely and re-visited by all staff and pupils at least annually.
- › 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.
- › 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

- › 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.

Practice

Management of eSafety eSafety in the curriculum

- › In order to be ready for the world of today, pupils need to understand the legal consequences of their online actions. See if topics such as terms and conditions, online payments and copyright can be integrated into the curriculum.
- › 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?
- › 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 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.esafetymodel.eu/group/community/embedding-online-safety-in-curriculum.

Extra curricular activities

- › Consider carrying out a simple survey in order to establish what pupils are doing when they go online. This will help to inform eSafety education within the school. Share your survey questionnaire and results in the eSafety Label community via your [My school area](#) (avoiding publishing any personal information) so that other schools can benefit from your work and even share their results with you for comparative purposes.

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.
- › Young people are more open to advice from their peers. Consider offering optional courses and/or school rewards on eSafety topics or similar that stimulate expert knowledge in pupils that then could become a point of reference for their peers.
- › Ask parents for feedback on the kind of eSafety support which is being provided for them and consider innovative ways to maximise the number of parents who are benefitting from, and accessing it. See the fact sheet Information for parents at www.esafetymodel.eu/group/community/information-for-parents to find resources that could be circulated to parents and ideas for parent evenings.

Staff training

- › 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](#).
- › It is important that teachers are aware 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. Ensure that all teachers are provided with information of this. 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.