

Action plan submitted by ŞERİFE YILDIRIM for Özel İdare 100. Yıl İlkokulu - 20.11.2020 @ 11:46:42

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

- › Your school system is not currently protected by a firewall. We recommend that you review this situation urgently and install a firewall for your school. It is essential to protect your school system from external intruders and from inappropriate internal use. Consult the fact sheet Protecting your devices against malware at [www.esafetylabel.eu/group/community/protecting-your-devices-against-malware](http://www.esafetylabel.eu/group/community/protecting-your-devices-against-malware).

### Pupil and staff access to technology

- › The fact that staff and pupils are allowed to use USB memory sticks in your school following permission, would require that all staff concerned receive adequate training to be able to know when they can be used safely. Is this the case? To keep your systems secure whilst allowing staff and pupils you also need to include the ground rules in your Acceptable Use Policy. Check the fact sheet on Use of removable devices at [www.esafetylabel.eu/group/community/use-of-removable-devices](http://www.esafetylabel.eu/group/community/use-of-removable-devices) to make sure you cover all security aspects.
- › Consider whether banning mobile devices is a rule that is fit for purpose and if your school might want to allow digital devices for some class activities. You could develop as part of your Acceptable Use Policy a section on how digital technologies can and cannot be used in the classroom; see the fact sheet on Using Mobile Phones at School ([www.esafetylabel.eu/group/community/using-mobile-device-in-schools](http://www.esafetylabel.eu/group/community/using-mobile-device-in-schools)).
- › The computer labs in your school are hard to book. Investigate if this can be facilitated and/or if there are other ways to facilitate usage of new media inside a lesson. Using digital devices is the best way to teach responsible use of new technologies to pupils. Consider whether using a BYOD (bring your own device) approach could work.
- › 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 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.
- › Having your learning and administration environments together can create a security risk. Ensuring security of staff's and pupils' private data is a fundamental role of the school. We recommend that your appointed eSafety manager/ICT coordinator, together with the staff and a technical expert, define and implement a strategy for separating learning and administration environments or ensuring the equivalent highest level of security between them. Read the fact sheet on Protecting sensitive data in schools at [www.esafetymodel.eu/group/community/protecting-sensitive-data-in-schools](http://www.esafetymodel.eu/group/community/protecting-sensitive-data-in-schools).

## Software licensing IT Management

- › Check your School Policy and the Acceptable Use Policy and update these if necessary to ensure that there is a clear authorisation process to be followed. The person in charge of the ICT network should be fully informed of what software is on school-owned hardware because s/he needs to be able to guarantee conformity with licensing requirements and that new software won't interfere with network operation.
- › It is good that staff members with questions about software issues can contact a school helpdesk. Consider whether you need to provide training and/or guidance to new software that is installed on school computers. This is important to ensure that school members will take advantage of new features, but also that they are aware of relevant security and data protection issues.
- › 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)

- › 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 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.
- › It is important that school policies are up-to-date. Ensure that a mechanism is in place which ensures that they are revised at least once a year. Also ensure that they are revised when changes that could affect them are put into place.

## 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](http://www.inhope.org)).
- › Ensure that all staff, including new members of staff, are aware of the guidelines concerning what to do if inappropriate or illegal material is discovered on a school machine. Ensure, too, that the policy is rigorously enforced. A member of the school's senior leadership team should monitor this.
- › Check that your School Policy includes all necessary information for teachers about handling issues when pupils knowingly or even inadvertently access illegal or offensive material online by going to the guidance set out by the [teachtoday.de/en](http://teachtoday.de/en) website ([tinyurl.com/9j86v84](http://tinyurl.com/9j86v84)). If such incidents arise in your school, make sure you anonymously fill out the eSafety Label Incident handling form ([www.esafetylabel.eu/group/teacher/incident-handling](http://www.esafetylabel.eu/group/teacher/incident-handling)) so that other schools can benefit from your experience.

## Staff policy

- › 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.
- › New technologies, such as smartphones or other mobile devices bring a new set of risks with them. Ensure that your teachers are aware of those. This way they can avoid the pitfalls when using the devices and also pass the knowledge onto the pupils.

## Pupil practice/behaviour School presence online

- › Having an official school page on some of the more widely used/popular social networking sites can be useful for parents, pupils and the broader public if you use it to publicise your actions and events. However, exercise care when setting this up to ensure that someone from the school has control over posts etc. Check the fact sheet on Schools on social networks ([www.esafetylabel.eu/group/community/schools-on-social-networks](http://www.esafetylabel.eu/group/community/schools-on-social-networks)) for further information.
- › Check the fact sheet on Taking and publishing photos and videos at school ([www.esafetylabel.eu/group/community/taking-and-publishing-photos-and-videos-at-school](http://www.esafetylabel.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

- › 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.esafetylevel.eu/group/community/school-policy](http://www.esafetylevel.eu/group/community/school-policy).

- › It is good that all staff in your school are responsible for eSafety. However, it is good practice to appoint a person who will have overall responsibility for eSafety issues to provide the focus needed. Ideally this should be someone from the senior leadership team. 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](http://www.esafetylevel.eu/group/teacher/incident-handling).

## 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.

## 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.esafetylevel.eu/group/community/pupils-use-of-online-technology-outside-school](http://www.esafetylevel.eu/group/community/pupils-use-of-online-technology-outside-school).
- › 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

- › Dobro je, da staršem nudite podporo v zvezi z e-varnostjo, ko si to želijo. Premislite, ali bi bilo dobro vse starše redno obveščati prek spletne strani ali prek povezav v šolskem e-glasilu. Morda imate lahko tudi roditeljski sestanek. Poglejte si smernice o informacijah za starše na [www.esafetylevel.eu/group/community/information-for-parents](http://www.esafetylevel.eu/group/community/information-for-parents), kjer boste našli gradiva, ki jih lahko posredujete staršem, in ideje, ki jih lahko uporabite na roditeljskih sestankih.

## 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](#).
- › 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?

- 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.esafetylevel.eu/group/community/suggestions-for-online-training-courses](http://www.esafetylevel.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.**