

Action plan submitted by Güldane BÜYÜKÇAM for Misak-ı Milli İlkokulu - 09.12.2019 @ 19:28:38

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 protected by a firewall. Ensure that the provision and management of the firewall are regularly reviewed and updated, as and when required.
- › 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.esafetylevel.eu/group/community/protecting-your-devices-against-malware.
- › 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.

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

- › 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.esafetylevel.eu/group/community/protecting-sensitive-data-in-schools).
- › 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.

- › Your school has a legal obligation under the Data Protection Act (DPA) 1998 to store, archive and dispose of personal information securely. Ensure that a good records management system is put in place. Check the according fact sheet for more information.

Software licensing

- › 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

- › 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.
- › 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)

- › 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 essential for all schools to have an Acceptable Use Policy (AUP) for staff and pupils. Consult with all stakeholders to draw up an AUP urgently. See the fact sheet and check list on Acceptable Use Policy at www.esafetylevel.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.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

- › Please share the materials in which you tackle these issues especially with pupils and parents in the of the eSafety Label portal.
- › It is good practice to log cyberbullying incidents that occur in your school centrally, as you are contributing to building a data base of successful incident handling practices from schools across Europe that you and others can use in future. Make sure that pupils sign up to anti-bullying guidelines in your Acceptable Use Policy.

Staff policy

- › In your school user accounts are managed in a timely manner. This is important as it decreases the risk of misuse.
- › Ensure that all staff understand the school's regulations on use of personal mobile devices in the classroom; these should be clearly communicated in the School Policy. Monitor the effectiveness of the policy and ensure that it is adhered to. You can also advise your staff to read the fact sheet Using mobile phones at school (www.esafetylabel.eu/group/community/using-mobile-device-in-schools).

Pupil practice/behaviour 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.
- › It is important that a designated member of staff has an overview of any social networking profiles set up by representatives of your school. 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. Consider setting up a school social media profile to facilitate monitoring and showcase initiatives and achievements, as this can be a useful dissemination tool.
- › We recommend that you specifically nominate a web-experienced staff member to periodically check the school's online reputation. Monitoring such an important aspect on an ad hoc basis only is insufficient. Remember that this is the image that prospective parents will receive when they search for your school online.

Practice

Management of eSafety

- › 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.esafetylabel.eu/group/teacher/incident-handling.

eSafety in the curriculum

- › 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 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.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum.

- › These issues are very topical at present and it is important to raise awareness and provide pupils with opportunities to discuss concerns and ask questions. Consider integrating some education around these issues into the overall eSafety 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](#).

Extra curricular activities

- › Use Safer Internet Day as a mechanism to get the whole school community involved with online safety. The information and resources available at www.saferinternetday.org offer an ideal opportunity to promote peer advocacy activities.
- › Gather feedback from pupils to see what sort of additional eSafety support they would benefit from outside curriculum time. Could they be involved in delivering some of this to their peers? Check the resource section on the eSafety Label portal to find resources that will help them do this; check out the fact sheet on Pupils' use of online technology outside school at www.esafetylabel.eu/group/community/pupils-use-of-online-technology-outside-school.

Sources of support

- › 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

- › 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?
- › 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](#).

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.