

Action plan submitted by Dilek BARDAKKAYA for SARAYBOSNA ANADOLU LİSESİ - 01.02.2023 @ 21:12:31

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](http://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 great that in your school laptops/tablets are easily accessible within a lesson. Using them provides best practise for pupils in dealing with new media. Ensure that safety issues are also discussed.
- › 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.

### 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.
- › 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

- › You need to make sure that all the software in your school is legally licensed and that copies of the licences are held centrally. You also need to check with whoever supports your IT systems that the software will not

compromise system security. Your school should develop a clear policy for software acquisition and it is good practice to centralise this process wherever possible.

- › It is good practise that the member of staff responsible is fully aware of installed software and their license status.
- › 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 practise that you are training and/or providing guidance in the use of new software that is installed on school computers. This ensures that school members will take advantage of new features, but also that they are aware of security and data protection issues where relevant.
- › 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](http://www.esafetylabel.eu/group/community/acceptable-use-policy-aup).

### 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.
- › 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)).
- › 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](http://www.esafetylabel.eu/group/teacher/incident-handling)), as this enables schools to share and learn from each other's strategies.

### Staff policy

- › In your school user accounts are adjusted within a weeks delay if the role of staff or pupil changes. Investigate if

this process could be optimised. The quicker that unused accounts are deactivated/adjusted, the less risk of misuse.

- 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?

## 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

- Review the policy on taking photographs of, and by, pupils, parents and staff and check that it reflects any recent developments. Ideally, the policy should focus on behaviour rather than specific technologies. 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](http://www.esafetylevel.eu/group/community/taking-and-publishing-photos-and-videos-at-school)) will provide a good starting point.
- 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.
- 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.esafetylevel.eu/group/community/schools-on-social-networks](http://www.esafetylevel.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.

# Practice

## Management of eSafety

- In addition to a clear designation of responsibility to ensure that all necessary network security and user privacy checks are in place, it is essential that schools also have audit and procedural checks at regular intervals. Without this, a school will be leaving itself vulnerable. See our fact sheet on School Policy at [www.esafetylevel.eu/group/community/school-policy](http://www.esafetylevel.eu/group/community/school-policy).

Although there should always be an overall lead person on eSafety just as you have in your school, everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties. Even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise problems. Use our fact sheet Acceptable Use Policy ([www.esafetylevel.eu/group/community/acceptable-use-policy-aup-](http://www.esafetylevel.eu/group/community/acceptable-use-policy-aup-)) to ensure that everyone plays their part in ensuring they are all the best and safest digital citizens they can be.

## eSafety in the curriculum

- › It is good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.
- › It is good practice that all pupils in all year groups in your school are taught about eSafety. It continues to be important to review regularly the curriculum provision to ensure it meets ever-changing needs. If you have a curriculum review process of this kind, it would be helpful to other schools if you could publish this on your school profile. To upload go to your [My school area](#).
- › 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 excellent that consequences of online actions are discussed with pupils in all grades. Terms and conditions need to be read to fully understand contractual conditions. This can also concern aspects of data privacy. Another important topic is breach of copyright. Please share the materials used through the uploading evidence tool, accessible also via the [My school area](#).
- › eSafety needs to be embedded across the whole curriculum regardless of whether this is a statutory obligation in your country. There are several very good schemes of work freely available which will support this; for further information see the fact sheet Embedding eSafety in the curriculum at [www.esafetymodel.eu/group/community/embedding-online-safety-in-curriculum](http://www.esafetymodel.eu/group/community/embedding-online-safety-in-curriculum).

## Extra curricular 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.esafetymodel.eu/group/community/pupils-use-of-online-technology-outside-school](http://www.esafetymodel.eu/group/community/pupils-use-of-online-technology-outside-school).
- › It is good to know that you are frequently using the online eSafety resources from your national Safer Internet Centre. Have you found these resources helpful in your school? Please send your feedback on their use and value to [info-insafe@eun.org](mailto:info-insafe@eun.org).

## 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

- › It should be a real benefit to your pupils that all staff receive regular training on eSafety issues. Continue to gather feedback from staff on the medium- and long-term benefits of the training and consult the eSafety Label portal to see suggestions for training courses at [www.esafetymodel.eu/group/community/suggestions-for-online-training-courses](http://www.esafetymodel.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.