

Action plan submitted by Esma ÇOLAK for 700.YIL OSMANGAZİ ORTAOKULU - 25.01.2021 @ 17:54:07

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

### Pupil and staff access to technology

- › 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)).
- › Since staff and pupils can use their own equipment on your school network, it is important to make sure that the Acceptable Use Policy is reviewed regularly by all members of the school and adapted as necessary. It must be discussed with pupils at the start of each academic year so that they understand what is in place to protect them and their privacy, and why. Base the policy around behaviour rather than technology. Visitors must also read and sign the Acceptable Use Policy before they use the school's network.

### 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.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools](http://www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools)).
- › It is good that your school records are stored in a safe environment, it is also necessary that they are archived and disposed with in line with the Data Protection Act. Ensure that a good records management system is put in place. Check the according fact sheet for more information.
- › 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.

## 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 practise that your 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.
- › 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.

# 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 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

- › 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.
- › 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.
- › 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.

## Staff policy

- › In your school user accounts are managed in a timely manner. This is important as it decreases the risk of misuse.

## Pupil practice/behaviour

- › 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.
- › 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

- › 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.
- › Regularly check the content of the school's online presence on social media sites to ensure that there are no inappropriate comments. Set up a process for keeping the site/page up to date, and check the fact sheet on Schools on social networks ([www.esafetymodel.eu/group/community/schools-on-social-networks](http://www.esafetymodel.eu/group/community/schools-on-social-networks)) for further information to make sure that good practice guidelines have been followed. Get feedback from stakeholders about how useful the profile is.

# Practice

## Management of eSafety 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.esafetymodel.eu/group/community/embedding-online-safety-in-curriculum](http://www.esafetymodel.eu/group/community/embedding-online-safety-in-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?

## Extra curricular activities

- › 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).

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

- › It is great that in your school pupils are actively encouraged to become eSafety mentors. You might want to share your approach to strengthening this network with other teachers on the eSafety Label website via the forum or your school's profile page, so that others can replicate it.
- › 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.esafetylabel.eu/group/community/information-for-parents](http://www.esafetylabel.eu/group/community/information-for-parents) to find resources that could be circulated to parents and ideas for parent evenings.
- › 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.**