

Action plan submitted by sevil kizmaz for şehit mustafa yaman anadolu imam hatip lisesi - 19.01.2023 @ 09:29:51

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](http://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.
- › 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

- › You should organise a meeting with other teachers so you can discuss how the school could use social media and digital devices as an aid to learning in the classroom. Look at the outcomes and report from the SMILE project (Social Media in Learning and Education, <http://www.eun.org/teaching/smile>) to learn more about using social media in the classroom.

### 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.
- › 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)).

## Software licensing

- › It is good practise that the member of staff responsible is fully aware of installed software and their license status.
- › 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 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.
- › 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.

# Policy

## Acceptable Use Policy (AUP)

- › It is good that you have an Acceptable Use Policy (AUP) for pupils. You should now amend the AUP to include staff and the wider community. To ensure that your revised 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

- › 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.
- › 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)).
- › Your teachers know how to recognise and handle (cyber)bullying. Think about ways to raise awareness also among pupils and parents. Check out the eSafety fact sheet for more information.

## Staff policy

- › In your school user accounts are managed in a timely manner. This is important as it decreases the risk of misuse.
- › 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](#).
- › 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](http://www.esafetylabel.eu/group/community/using-mobile-device-in-schools)).

## Pupil practice/behaviour

- › When discussing eSafety pupils at your school can sometimes provide feedback on the activities. Involve them as much as possible so that the teacher recognises real life issues while the pupils are more engaged.

## School presence online

- › 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.
- › 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.

# Practice

## Management of eSafety

- › It is good that you have a designated member of staff responsible for eSafety. Consider whether it would be helpful to have an eSafety committee comprising members from all groups of stakeholders. 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](http://www.esafetylabel.eu/group/teacher/incident-handling).
- › In your school, teachers are responsible for their own pupils' online activity. There are many network security and user privacy, audit and procedural tool checks and balances that need to take place to ensure the safety of your pupils and the school networks, and these should be laid down in your School Policy. See our fact sheet on School Policy at [www.esafetylabel.eu/group/community/school-policy](http://www.esafetylabel.eu/group/community/school-policy).

To ensure this happens as efficiently and often as necessary, we advise that the Principal of your school appoints one individual staff member to look after eSafety management in the school. This person will be responsible for seeing that all aspects included in your School Policy are discussed and looked at with other

teachers as well as with pupils in the classroom.

To ensure that every staff member, pupil and parent is aware of her or his online rights and responsibilities, see the fact sheet on Acceptable Use Policy ([www.esafetylabel.eu/group/community/acceptable-use-policy-aup-](http://www.esafetylabel.eu/group/community/acceptable-use-policy-aup-)).

## eSafety in the curriculum

- › 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.
- › 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 that these issues have been included in the eSafety curriculum. It is a good idea to regularly review the issues which are being covered by your eSafety education in order to ensure that new and emerging issues are covered.

## Extra curricular activities Sources of support

- › 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.

## 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?
- › 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.esafetylabel.eu/group/community/suggestions-for-online-training-courses](http://www.esafetylabel.eu/group/community/suggestions-for-online-training-courses).
- › 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 good practise that you provide information to teachers 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. You might want to 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.