

Action plan submitted by Meliha Erdoğan for Halis Gülle Anadolu Lisesi - 19.01.2023 @ 18:49:06

**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.
- › 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 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.
- › All staff and pupils are allowed to use USB memory sticks in your school. This is good practice, and your Acceptable Use Policy should stipulate that all removable media is checked before use in the school systems. 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.
- › 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

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

## 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.
- › Once a year decisions on new hard/software are made. Investigate ways to also allow for new hard/software requests throughout the year. It will allow teachers to create a more engaging lesson without the temptation of unauthorized copying and its inherent dangers and costs.

## Policy

### Acceptable Use Policy (AUP)

- › 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.
- › Regularly review the Mobile Phone Policy to ensure that it is fit for purpose and that it is being applied consistently across the school. The fact sheets on Using mobile phones at school ([www.esafetylevel.eu/group/community/using-mobile-device-in-schools](http://www.esafetylevel.eu/group/community/using-mobile-device-in-schools)) and School Policy ([www.esafetylevel.eu/group/community/school-policy](http://www.esafetylevel.eu/group/community/school-policy)) will provide helpful information.

### 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.
- › 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

- › There are dangers associated with the use of personal mobile devices in class. Consider why staff would need to use their device and, if appropriate, consider providing a school device. Advise staff to read 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)) and ensure that the guidelines to staff are clearly communicated in the School Policy.

- 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

- 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.
- You have defined electronic communication guidelines in your Acceptable Use Policy and this would be a useful example of good practice for other schools. Can you create a tutorial about electronic communication guidelines for pupils and upload it to your school profile via your [My school area](#) so that other schools can benefit from your experience.

## School presence online

- 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.esafetylabel.eu/group/community/schools-on-social-networks](http://www.esafetylabel.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.
- 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.

# Practice

## Management of eSafety

- It is good that the job description outlines that the member of staff responsible for ICT needs to keep up to date with new technologies. In addition, it would be good to regularly send the ICT responsible to trainings/conferences so (s)he can keep up with new features and risks. Check out the [Better Internet for Kids portal](#) to stay up to date with the latest trends in the online world.
- 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.esafetylabel.eu/group/community/school-policy](http://www.esafetylabel.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.esafetylabel.eu/group/community/acceptable-use-policy-aup-](http://www.esafetylabel.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 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 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](#).
- › 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.
- › It is good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.

## Extra curricular activities 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.
- › All staff should have some responsibility for eSafety. School counsellors, nurses, etc. are all well placed to provide advice and guidance on these issues and should be invited to contribute to developing and regularly reviewing your School Policy. Make the maximum use of their knowledge and skills and consider whether it is appropriate to provide training for them.

## Staff training

- › 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.