

Action plan submitted by Reyhan VAHAPOĞLU for Silopi Atatürk Anadolu Lisesi - 19.01.2023 @ 08:50:36

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 for examples of discussions that can take place in the classroom on this topic, through role-play and group games.
- › 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.

Pupil and staff access to technology

- › 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.esafetylevel.eu/group/community/use-of-removable-devices to make sure you cover all security aspects.
- › There are clear advantages for staff and pupils to bring their personal devices to school and to access internet on them. Besides supplementing the technical equipment available at school, this provides an important link between learning at home and at school and an opportunity to guide young people in responsible use. However, staff and pupil use of their own equipment on the school network needs to be addressed in an Acceptable Use Policy so that users are clear about which networks they should use and why. The Acceptable Use Policy needs to include clear guidance about which activities are permitted while on the school network, and what is not allowed.

Data protection

- › It is good that your school provides materials on the importance of protecting devices, especially portable ones. Ensure that staff are aware of these and use them. This material should be pointed out to new staff as part of their induction. Please consider uploading those as evidence at [evidence](#) and sharing with others in the forum. 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.
- › It is good that all users are attributed a different password by the system in your school. Remind all school members never to write their given password down anywhere, certainly not on a sticker on a computer! Also, ensure that the Acceptable Use Policy reminds staff and pupils to keep their passwords secure and not share them with others.

Software licensing 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.
- › 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)

- › 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) and School Policy (www.esafetylevel.eu/group/community/school-policy) will provide helpful information.
- › 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-
- › School policies and procedures are essential to ensure a smooth operation within a school and that all school members follow the same set of rules and guidelines. Ensure that school policies exist and that all school members are aware of them. You can find more information on this in the of the eSafety Label website.
- › 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.

Reporting and Incident-Handling

- › 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).
- › 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), as this enables schools to share and learn from each other's strategies.

Staff policy

- › There should be a code of conduct for staff so that they are clear about what is acceptable behaviour when they are online. This should be clearly communicated to all staff in the School Policy, and to staff and pupils in the Acceptable Use Policy. Regularly review and update both documents as necessary.
- › 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](#).

Pupil practice/behaviour 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) 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

- › 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.

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-) to ensure that everyone plays their part in ensuring they are all the best and safest digital citizens they can be.

- › Consider appointing a governor or board member who provides a liaison for eSafety issues. Consider also reporting on the number and type of eSafety incidents to the governing body on an annual basis when you also review your School Policy. See our fact sheet on School Policy www.esafetylevel.eu/group/community/school-policy.

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 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](#).
- › 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?
- › 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](#).

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.

Sources of support

- › Young people are more open to advice from their peers. Consider offering optional courses and/or school rewards on eSafety topics or similar that stimulate expert knowledge in pupils that then could become a point of reference for their peers.

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?
- › All staff need to be regularly updated about emerging trends in eSafety issues. Consider a needs-analysis to

determine what different staff need from their training and consult the eSafety Label portal to see suggestions for training courses at www.esafetylabel.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.