

Action plan submitted by azize taşar çelikdöğen for Serik Gazi Ortaokulu - 16.01.2023 @ 10:50:05

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 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

- › 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.
- › 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.
- › 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.esafetylevel.eu/group/community/using-mobile-device-in-schools).

Data protection

- › You have a good policy of encrypting pupil data and storing it safely. Ensure all new staff made aware of the procedures for encryption and data handling and that there is a named point of contact acting as the data controller for your school. Upload to your school profile some guidelines about protecting sensitive data through

an encryption system so that other schools can benefit from your experience.

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 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.
- › In your school only the head master and/or IT responsible can acquire new software. Consider putting a system into place where teachers can ask for new software in a non-bureaucratic and timely fashion. This allows teachers to create a more engaging lesson without the temptation of unauthorized copying and its inherent dangers and costs.
- › 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.

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.

Reporting and Incident-Handling

- › It is important to have a school-wide policy on handling issues when pupils knowingly or even inadvertently access illegal or offensive material online, since standards and practices can vary considerably from one teacher to the next. Guidance on this topic is provided on the teachtoday.de/en website (tinyurl.com/9j86v84). If such incidents arise in your school, make sure you anonymously fill out the eSafety Label Incident handling form (www.esafetylevel.eu/group/teacher/incident-handling) so that other schools can benefit from your experience.
- › 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.
- › Online issues that take place outside of school will inevitably have an impact inside school. Consider whether the school needs to make a statement about how such issues will be dealt with in the School Policy and the Acceptable Use Policy. Don't forget to anonymously document incidents on the Incident handling form

(www.esafetylevel.eu/group/teacher/incident-handling), as this enables schools to share and learn from each other's strategies.

Staff policy

- › 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](#).
- › 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.
- › 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

- › It is good that pupils can give feedback on the school's online presence. Think about creating a space that is entirely managed by pupils. It's a great opportunity to learn about media literacy and related issues. It also can help to establish a peer network of support. Find out more about in the eSafety Label fact sheet.
- › Check 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) 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.

Practice

Management of eSafety

- › Ensure that the governor or board member appointed for eSafety has the opportunity to receive regular training and also to ensure that colleagues are aware of eSafety issues. Involve your governing body in the development and regular review of your School Policy. See our fact sheet on School Policy www.esafetylevel.eu/group/community/school-policy.

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 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 practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.

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.
- › Consider offering pupils support to deal with online safety issues they meet outside school and make a note of these to share with other schools in the eSafety Label community. It may be helpful to provide a “surgery” to help pupils to set their Facebook privacy, etc. The eSafety Label portal provides resources that will be useful for this; check out the fact sheet on Pupils' use of online technology outside school at www.esafetymlabel.eu/group/community/pupils-use-of-online-technology-outside-school.

Sources of support

- › Dobro je, da staršem nudite podporo v zvezi z e-varnostjo, ko si to želijo. Premislite, ali bi bilo dobro vse starše redno obveščati prek spletne strani ali prek povezav v šolskem e-glasilu. Morda imate lahko tudi roditeljski sestanek. Poglejte si smernice o informacijah za starše na www.esafetymlabel.eu/group/community/information-for-parents, kjer boste našli gradiva, ki jih lahko posredujete staršem, in ideje, ki jih lahko uporabite na roditeljskih sestankih.
- › 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.

Staff training

- › 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.esafetymlabel.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](#).

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.