

Action plan submitted by Zehra ÇELİK for 1071 MALAZGİRT İLKOKULU - 12.02.2023 @ 14:55:59

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.esafetymalware.eu/group/community/protecting-your-devices-against-malware.
- › 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

- › 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.esafetymalware.eu/group/community/use-of-removable-devices to make sure you cover all security aspects.
- › The computer labs in your school are hard to book. Investigate if this can be facilitated and/or if there are other ways to facilitate usage of new media inside a lesson. Using digital devices is the best way to teach responsible use of new technologies to pupils. Consider whether using a BYOD (bring your own device) approach could work.

Data protection

- › 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.
- › Your new users are given a standard password and are asked to generate their own password on their first

access. Passwords offer unique entry points into the school computing system and some basic rules of password security should be rigorously applied. For further information, read the fact sheet on Safe passwords at www.esafetylabel.eu/group/community/safe-passwords.

Include these rules in your Acceptable User Agreement and avoid giving new users a standard "first access" password.

Software licensing

- › Review the budget for software needs. You might also want to look into alternatives, e.g. Cloud services or open software.
- › 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

- › 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 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)

- › When other school policies are reviewed, consider whether it would be appropriate to make references to eSafety, bearing in mind the wide range of issues that eSafety covers.
- › 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?
- › This is good teaching practice, but you need to consolidate it with a section dedicated to mobile phone usage in your School Policy and your Acceptable Use Policy. Consult all stakeholders to develop this; the fact sheets on Using mobile phones at school (www.esafetylabel.eu/group/community/using-mobile-device-in-schools) and School Policy (www.esafetylabel.eu/group/community/school-policy) will provide helpful information.

Reporting and Incident-Handling

- › Have teachers received training on dealing with potentially illegal material? Is the procedure clearly indicated in the School Policy and the Acceptable Use Policy which all teachers and pupils have signed? All staff and pupils

should be aware that they should report any suspected illegal content to the national INHOPE hotline (www.inhope.org).

- › It is important to have a clearly communicated School Policy on this, and it should be mentioned in the Acceptable Use Policy too. What is considered to be potentially illegal can vary from person to person, so it is important that this is discussed with staff members and that school standards are set. All members of the school including pupils and teachers must be informed of them and required to respect them.
- › 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.
- › 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

- › In order to decrease the risks of misuses of user accounts, ensure that you put a procedure in place that immediately informs the ICT responsible to adjust user rights and/or deactivate them if the role of staff or pupil has changed.
- › 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) and ensure that the guidelines to staff are clearly communicated in the School Policy.

Pupil practice/behaviour 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.

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.esafetylabel.eu/group/community/school-policy.

eSafety in the 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.

- › 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
- › While it is good that you discuss consequences of online actions terms and conditions, online payments and copyright with older pupils, consider discussing these also with young pupils.
- › 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.
- › You may want to consider including sexting in your child protection policy to help to ensure a consistent whole-school approach to dealing with any incidents.
- › 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](#).

Extra curricular activities

- › Try to develop further the engagement of pupils in peer mentoring and provide them with more opportunities to share their thoughts and understanding with their peers. Also check out the resource section of the eSafety Label portal to get further ideas and resources.

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.esafetymodel.eu/group/community/information-for-parents, kjer boste našli gradiva, ki jih lahko posredujete staršem, in ideje, ki jih lahko uporabite na roditeljskih sestankih.
- › 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

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.