

Action plan submitted by Zeynep Gizem Emir for Atatürk İlkokulu - 18.01.2023 @ 13:32:49

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

- You urgently need to get virus protection for devices that need to be protected on the school network since only some of them are protected at the moment. Just one infected device can contaminate the school's whole network and certain types of virus can even save illegal content to your server.
You should also include 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. Check out the fact sheet on Protecting your devices against malware at www.esafetylevel.eu/group/community/protecting-your-devices-against-malware.
- It is important that your ICT services are regularly reviewed, updated and removed if no longer in use. Installing the latest versions and patches often addresses security vulnerabilities without which your services might come under attack. Ensure that this is part of the job description of the ICT coordinator.
- Your school system is protected by a firewall but is sometimes bypassed for certain applications. While there may be some arguments for bypassing it, it is usually inadvisable to do so. If it is decided that the school policy will permit this, then it should only be implemented by an authorised technical manager and then on a restricted time basis.

Pupil and staff access to technology Data protection

- 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.
- 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.
- Having your learning and administration environments together can create a security risk. Ensuring security of staff's and pupils' private data is a fundamental role of the school. We recommend that your appointed eSafety

manager/ICT coordinator, together with the staff and a technical expert, define and implement a strategy for separating learning and administration environments or ensuring the equivalent highest level of security between them. Read the fact sheet on Protecting sensitive data in schools at www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools.

Software licensing

- › 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.
- › 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

- › 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.
- › 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.

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.
- › 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.
- › 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?

Reporting and Incident-Handling

- › It is a pity not to share the details and solutions applied to bullying incidents both with the staff members and via the eSafety Label incident handling form. Only in this way can you learn through experience and the successful

incident handling practices of others. You should also make sure that anti-bullying guidelines are given to pupils and staff 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.
- › 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

- › 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?
- › In your school user accounts are managed in a timely manner. This is important as it decreases the risk of misuse.

Pupil practice/behaviour

- › 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

Practice

Management of eSafety eSafety in the curriculum

- › Cyberbullying is one of the key issues that helplines are contacted about and can have a devastating effect on pupils' lives. Discuss the topic with pupils from a very early age, maybe in the form of role plays. Also check out the fact sheet on [Cyberbullying](#) for more information.

- › Although these are sensitive issues, it is good to be proactive about raising awareness of them. Consider integrating some education around these issues into the overall eSafety curriculum.
- › 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.
- › 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

Extra curricular activities

- › Consider carrying out a simple survey in order to establish what pupils are doing when they go online. This will help to inform eSafety education within the school. Share your survey questionnaire and results in the eSafety Label community via your [My school area](#) (avoiding publishing any personal information) so that other schools can benefit from your work and even share their results with you for comparative purposes.
- › 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

- › There is a school counselor in your school though not trained on eSafety issues. Investigate if there is a training course that this teacher could follow in order to be better equipped to help pupils dealing with issues related to new media.
- › 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.
- › It is good that there is an informal network of 'eSafety expert' pupils in your school. Explore ways to strengthen this, maybe through optional courses and/or school rewards on eSafety topics or similar.

Staff training

- › It is important that teachers are aware 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. Ensure that all teachers are provided with information of this. 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.