eSafety Label - Action Plan

Action plan submitted by Halil İbrahim ÖZMEN for İnlice Ahmet Nazif Zorlu İlkokulu-Ortaokulu - 17.01.2023 @ 11:35:54

> 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.

> It is good practice that your ICT services are regularly reviewed, updated and removed if no longer in use.

> 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

> 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.esafetylabel.eu/group/community/using-mobile-device-in-schools).

> 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.esafetylabel.eu/group/community/use-of-removable-devices to make sure you cover all security aspects.

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

> Ensure that all staff are aware of the procedure for purchasing new software and that all licenses are appropriate for the number of pupils and staff that will be using them. The End-user license agreement section in Wikipedia will provide useful information for understanding terms and conditions and comparing software agreements.

> 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)

> 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

> Keep a central log of any cyberbullying incidents which will help to inform staff about the extent of any potential issues and the type of pupil, age etc. that are affected. Also, be sure that you fill in the eSafety Label Incident handling form. Your input will contribute to building a data base of successful incident-handling practices from schools across Europe that you can use in the future.

> 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.

> Consider making the policy on 'Online incidents that take place outside school' more explicit and ensure that it is clearly communicated to all through the School Policy and the Acceptable Use Policy. 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.

> 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.

> 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).

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

> 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.

> Your school has a school wide approach of positive and negative consequences for pupil behaviour. This is good practice, please share your policy via the My school area of the eSafety portal so that other schools can learn from it.

School presence online

Practice

Management of eSafety

> It is good that all staff in your school are responsible for eSafety. However, it is good practice to appoint a person who will have overall responsibility for eSafety issues to provide the focus needed. Ideally this should be someone from the senior leadership team. Ensure that this person is involved in the development and regular review of your School Policy. She or he should not only be informed, but should also fill out the Incident handling form whenever an incident arises at www.esafetylabel.eu/group/teacher/incident-handling.

eSafety in the 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 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.

> eSafety needs to be embedded across the whole curriculum regardless of whether this is a statutory obligation in your country. There are several very good schemes of work freely available which will support this; for further information see the fact sheet sheet Embedding eSafety in the curriculum at www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum.

> 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

> How do you organise peer mentoring among pupils on eSafety? Check out the resources of the ENABLE project and share your ideas in the forum of the eSafety Label community so that other schools can benefit from your experience to establish a similar approach.

> Consider sharing the information you have about your pupils' online habits with other schools through the eSafety Label community. You could, for example, upload your latest survey findings on pupils' online habits to your school profile via your My school area.

Sources of support 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?

> It should be a real benefit to your pupils that all staff receive regular training on eSafety issues. Continue to gather feedback from staff on the medium- and long-term benefits of the training and consult the eSafety Label portal to see suggestions for training courses at www.esafetylabel.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.