eSafety Label - Action Plan

Action plan submitted by İsmail Hakkı GÜLEÇ for GEDİZ MESLEKİ ve TEKNİK ANADOLU LİSESİ - 16.01.2023 @ 12:53:01

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 Pupil and staff access to technology

> Ensure that the policy on mobile phones is being applied consistently throughout the school. Take a look at the fact sheet on Using Mobile Phones at School (www.esafetylabel.eu/group/community/using-mobile-device-in-schools).

> It is great that in your school laptops/tablets are easily accessible within a lesson. Using them provides best practise for pupils in dealing with new media. Ensure that safety issues are also discussed.

> All staff and pupils are allowed to use USB memory sticks in your school. This is good practice, and your Acceptable Use Policy should stipulate that all removable media is checked before use in the school systems. 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

> 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.

> It is good that your email system is protected and that you have a policy for the transfer of pupil data in place. In this regard, it is important to draw up guidelines so that all staff are clear about what to do if they discover inappropriate or illegal content on school machines. For further information see the fact sheet on Protecting sensitive data (www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools).

> 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 your school provides training materials on the importance of protecting devices, especially portable ones. Please consider sharing those with others through the in . Also ensure that your materials are regularly reviewed to ensure they are in line with the state of the latest technology.

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.

> Keeping track of installed software and its licenses is a crucial task in order to avoid expired software licenses and to remain legal within the school ICT infrastructure. Ensure there is is an ICT responsible who will be able to produce an overview at any given moment.

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.

Policy

Acceptable Use Policy (AUP)

> 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?

> It is good that school policies are reviewed annually in your school. Ensure that they are also updated when changes are put into place that could affect them. All staff should be aware of the contents of the policy.

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.

> 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?

> Ensure that all staff understand the school's regulations on use of personal mobile devices in the classroom; these should be clearly communicated in the School Policy. Monitor the effectiveness of the policy and ensure that it is adhered to. You can also advise your staff to read the fact sheet Using mobile phones at school (www.esafetylabel.eu/group/community/using-mobile-device-in-schools).

Pupil practice/behaviour

> 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.

> Electronic communication guidelines for pupils should be clearly communicated in the Acceptable Use Policy. Communication between pupils can rapidly degenerate if school-wide standards are not set, giving rise to incidents such as cyberbullying. Learning about effective, responsible communication should also be part of the school curriculum, as it is a necessary competence for every young person. Discuss this at a staff meeting in order to define the standards you want to implement.

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

> It is good that the job description outlines that the member of staff responsible for ICT needs to keep up to date with new technologies. In addition, it would be good to regularly send the ICT responsible to trainings/conferences so (s)he can keep up with new features and risks. Check out the Better Internet for Kids portal to stay up to date with the latest trends in the online world.

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.

> In your school older pupils are taught about the responsibilities and consequences when using social media. In today's times, younger and younger children are using social media. Consider therefore, to extend lessons on these topics also to younger pupils.

> 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 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 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.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum.

> 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 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.

> It is great that you have a staff member which is knowledgable in eSafety issues who acts as a teacher of confidence to pupils.

Staff training

> It is good practise that you provide information to teachers 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. You might want to 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.