eSafety Label - Action Plan

Action plan submitted by YASEMİN EŞMELİOĞLU for YAHYA KEMAL ORTAOKULU - 09.03.2024 @ 19:48:01

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

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

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.
- 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).

Data protection

- 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).
- 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.

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 is good practise that the member of staff responsible is fully aware of installed software and their license status.

IT Management

- 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.

- 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)

- School policies and procedures are essential to ensure a smooth operation within a school and that all school members follow the same set of rules and guidelines. Ensure that school policies exist and that all school members are aware of them. You can find more information on this in the of the eSafety Label website.

- It is essential for all schools to have an Acceptable Use Policy (AUP) for staff and pupils. Consult with all stakeholders to draw up an AUP urgently. See the fact sheet and check list on Acceptable Use Policy at www.esafetylabel.eu/group/community/acceptable-use-policy-aup-.

Reporting and Incident-Handling

- Accessing illegal material may in itself be an illegal act. It is essential that staff are told exactly what they must do if pupils knowingly or inadvertently access illegal or offensive material online. You can find clear guidance on how to develop your policy regarding this issue on the teachtoday.de/en website (direct link:tinyurl.com/9j86v84). If such incidents arise in your school, make sure you anonymously fill out the eSafety Label Incident handling form (www.esafetylabel.eu/group/teacher/incident-handling) so that other schools can benefit from your experience.

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

- 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.

- 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.

Staff policy

- In order to decrease the risks of misues 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.

Pupil practice/behaviour

- 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

- We recommend that you specifically nominate a web-experienced staff member to periodically check the school's online reputation. Monitoring such an important aspect on an ad hoc basis only is insufficient. Remember that this is the image that prospective parents will receive when they search for your school online.

- Check the fact sheet on Taking and publishing photos and videos at school (www.esafetylabel.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

- In your school, teachers are responsible for their own pupils' online activity. There are many network security and user privacy, audit and procedural tool checks and balances that need to take place to ensure the safety of your pupils and the school networks, and these should be laid down in your School Policy. See our fact sheet on School Policy at www.esafetylabel.eu/group/community/school-policy.
  To ensure this happens as efficiently and often as necessary, we advise that the Principal of your school appoints one individual staff member to look after eSafety management in the school. This person will be responsible for seeing that all aspects included in your School Policy are discussed and looked at with other teachers as well as with pupils in the classroom.
  To ensure that every staff member, pupil and parent is aware of her or his online rights and responsibilities, see the fact sheet on Acceptable Use Policy (www.esafetylabel.eu/group/community/acceptable-use-policy-aup-).

eSafety in the curriculum

- 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 important that children understand responsibilities and consequences when using social media. Discuss with your teachers how this could be integrated into lessons. Topics should include issues such as digital footprints and data privacy.

- eSafety needs to be embedded within the 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 Embedding eSafety in the curriculum at www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum.

Extra curricular activities

- Use Safer Internet Day as a mechanism to get the whole school community involved with online safety. The information and resources available at www.saferinternetday.org offer an ideal opportunity to promote peer advocacy 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.

- 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.esafetylabel.eu/group/community/pupils-use-of-online-technology-outside-school.

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.

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

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.