eSafety Label - Action Plan

Action plan submitted by İlhan ÇELİK for HALİDE HATUN İLKOKULU - 12.01.2021 @ 10:07:28

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.

- Your school system is not currently protected by a firewall. We recommend that you review this situation urgently and install a firewall for your school. It is essential to protect your school system from external intruders and from inappropriate internal use. Consult the fact sheet Protecting your devices against malware at www.esafetylabel.eu/group/community/protecting-your-devices-against-malware.

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.

- You should organise a meeting with other teachers so you can discuss how the school could use social media and digital devices as an aid to learning in the classroom. Look at the outcomes and report from the SMILE project (Social Media in Learning and Education, http://www.eun.org/teaching/smile) to learn more about using social media in the classroom.

- 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

- Unprotected devices and even more so portable devices are a very high risk to data protection and not just to the device owner itself, but also to any person he has contact with. It is therefore crucial that all staff are informed and that this is also explained to pupils. Consider producing materials to share with all of your staff that raises awareness on this issue. This material should also be pointed out to new staff as part of there induction.

- 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

- 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.

- 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.

- 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.

IT Management

Policy

Acceptable Use Policy (AUP)

- 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

- 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.

- 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

- Ensure that all staff, including new members of staff, are aware of the policy concerning online conduct. This should be a topic that is regularly discussed at staff meetings and clearly communicated in the School Policy, and to staff and pupils in the Acceptable Use Policy. Regularly review and update both documents as necessary.

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

- 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

- When discussing eSafety pupils at your school can sometimes provide feedback on the activities . Involve them as much as possible so that the teacher recognises real life issues while the pupils are more engaged.

School presence online

- It is a pity that your school does not have an online presence. An online school presence can be a powerful tool to communicate with pupils, parents and teachers. Find out more about in the eSafety Label fact sheet.

- You have a dedicated person to monitor your school's online reputation, and this is good practice. Always be aware of any new sites that may not be immediately apparent through a regular search. Keep up to date with the latest sites and monitor these periodically, as they can be particularly damaging for schools and their pupils and staff if they present a negative viewpoint.

- Regularly check the content of the school's online presence on social media sites to ensure that there are no inappropriate comments. Set up a process for keeping the site/page up to date, and check the fact sheet on Schools on social networks (www.esafetylabel.eu/group/community/schools-on-social-networks) for further information to make sure that good practice guidelines have been followed. Get feedback from stakeholders about how useful the profile is.

Practice

Management of eSafety

- In addition to a clear designation of responsibility to ensure that all necessary network security and user privacy checks are in place, it is essential that schools also have audit and procedural checks at regular intervals. Without this, a school will be leaving itself vulnerable. See our fact sheet on School Policy at www.esafetylabel.eu/group/community/school-policy.
  Although there should always be an overall lead person on eSafety just as you have in your school, everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties. Even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise problems. Use our fact sheet Acceptable Use Policy (www.esafetylabel.eu/group/community/acceptable-use-policy-aup-) to ensure that everyone plays their part in ensuring they are all the best and safest digital citizens they can be.

- It is good that you have a designated member of staff responsible for eSafety. Consider whether it would be helpful to have an eSafety committee comprising members from all groups of stakeholders. 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

- Ensure that the eSafety curriculum keeps up with emerging issues by making full use of all available resources and ensure that it builds on prior learning, bearing in mind that pupils will need different messages depending on how they are using the technology.

- 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 good that you are making a specific reference to sexting within your child protection policy as this is a growing issue that many young people are having to deal with. It is also important to ensure that you are providing appropriate education for pupils about this issue.

Extra curricular activities

- Try to engage pupils in peer mentoring and provide them with 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

- Premislite, ali bi bilo dobro vse starše redno obveščati o zadevah glede e-varnosti 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.

- 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

- 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.

- All teachers should be able to recognise signs of cyberbullying and be aware on how to best proceed. Make sure that your teachers are regularly trained bearing in mind the rapid changes of new technology. Also check the eSafety fact sheet on Cyberbullying at www.esafetylabel.eu/group/community/cyberbullying.

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.