eSafety Label - Action Plan for: HRISTO SMIRNENSKI PRIMARY SCHOOL

Assessment form was submitted by: Deyana Peykova - 2014-11-28 17:41:38

Infrastructure

Technical security

- It is very good that all your school computers are virus-protected. Make sure you also have included 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. If you need further information, check out the fact sheet on Protecting your devices against malware at www.esafetylabel.eu/group/teacher/protecting-devices-against-malware.
- You have differentiated levels of filtration, which is excellent policy. A good policy should regularly update - so is it in your case? How often do you have requests for blocking or unblocking sites? Consider whether it is productive and engage all stakeholders. Note that the key to safe and responsible online behavior is a pedagogical approach to skills for online safety among students. Organize a meeting with all teachers and discuss how each to speak to their students how to be good citizens and protection of digital space. Look www.paneuyouth.eu for example discussions on the topic, which can make through role or group games.

Pupil and staff access to technology

- 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/teacher/removable-devices to make sure you cover all security aspects.

- There are clear advantages for the school team, and for students, when they use personal devices at school. This enriches the technical equipment available at school and is also a way to educate young people about responsible use.
  It is important when teachers and students use personal devices in the school to understand better which network to use and why.

-

Data protection

- It is good that you have separate servers for educational and administrative needs. Make sure that school team is prepared to manage those bases. Share your rules with other schools.

- Passwords offer a unique method of entry into the school computer system and has basic rules which must be strictly applied. For further information, read the information brochure Topic Reliable passwords www.esafetylabel.eu/group/teacher/safe-passwords

Software licensing

- It is important to ensure that all new staff are briefed about the effective processes you have for the installation of new software. This will mean that the security of your systems can be maintained and that staff can try out new software applications that will help teaching and learning.

- 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

- 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)

- The existence of rules about using ICT for pupils is commendable. You have to expand it in order to cover school team and the wider school community.
- Regularly review the ordinance for mobile phones, to make sure that it is valid and that is respected.

Reporting and Incident-Handling

- Have teachers received training on dealing with potentially illegal material? Is the procedure clearly indicated in the School Policy and the Acceptable Use Policy which all teachers and pupils have signed? All staff and pupils should be aware that they should report any suspected illegal content to the national INHOPE hotline (www.inhope.org).

- 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.

Staff policy

- There should be a code of conduct for staff so that they are clear about what is acceptable behaviour when they are online. This should be clearly communicated to all staff in the School Policy, and to staff and pupils in the Acceptable Use Policy. Regularly review and update both documents as necessary.

- There are dangers associated with the use of personal mobile devices in class. Consider why staff would need to use their device and, if appropriate, consider providing a school device. Advise staff to read the fact sheet on Using mobile phones at school (www.esafetylabel.eu/group/teacher/mobile-phones) and ensure that the guidelines to staff are clearly communicated in the School Policy.

Pupil practice/behaviour

- Guidelines for permissible electronic communication should be included in the Rules for use of ICT The lack of clear standards can lead to increased incidence of violence and bullying between peers.

- Your school partly has a school wide approach of positive and negative consequences for pupil behaviour. This is a good start, make sure that the policy and associated hierarchy applies to all on- and offline issues and is shared widely and re-visited by all staff and pupils at least annually.

School presence online

- C h e c k t h e f a c t s h e e t o n T a k i n g a n d p u b l i s h i n g p h o t o s a n d v i d e o s a t s c h o o l (www.esafetylabel.eu/group/teacher/photos-videos) 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.
- 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/teacher/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

- It is important that schools regularly conduct audits and inspections. Without them the school will become vulnerable. Explore our information brochures on the topic School Rules at www.esafetylabel.eu/group/teacher/school-policy
  There must always be person responsible for online safety, but both you and the school must share a common responsibility to protect any "sensitive" information used in the performance of their daily duties. Even people whose duties are not directly related to the use
  data must be acquainted with the risks and security measures. Use our information Rules for use brochure, (www.esafetylabel.eu/group/teacher/acceptable-use-)

- Consider appointing a governor or board member who provides a liaison for eSafety issues. Consider also reporting on the number and type of eSafety incidents to the governing body on an annual basis when you also review your School Policy. See our fact sheet on School Policy www.esafetylabel.eu/group/teacher/school-policy.

eSafety in the curriculum

- It is important that children understand the responsibilities and consequences when using social media (e.g. Facebook, Blogs, Instagram, Google+, etc). See with your teachers how this could be integrated into the lessons. Topics would include digital footprint, data privacy.

Extra curricular activities

- It is good that you provide eSafety support for your pupils outside curriculum time when asked. Consider offering all pupils support to deal with online safety issues. 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/teacher/social-media-pupils.

Sources of support

- All staff should have some responsibility for eSafety. School counsellors, nurses etc. are well placed to provide advice and guidance on these issues and should be invited to contribute to developing and regularly reviewing your School Policy. Consider whether it is appropriate to provide training for these staff.

- It is good that you provide eSafety support for parents when asked. Consider providing regular information for all parents through the school website or by providing links in a school newsletter. It may be possible to run a parent information evening. See the fact sheet Information for parents at www.esafetylabel.eu/group/teacher/info-forparents to find resources that could be circulated to parents and ideas for parent evenings.

Staff training

- 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/teacher/cyberbullying.

- The team should be informed about the trends in children online beahviour. Analyze training needs of the school team and meet training opportunities www.esafetylabel.eu/group/teacher/esafety-training-courses.