eSafety Label - Action Plan

Action plan submitted by SEMRAN KAYA for Alper Duru Anaokulu - 16.01.2021 @ 08:45:21

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

- You have differentiated levels of filtering in your school which is an excellent policy. A good policy still needs to be regularly updated - is the system being regularly updated? How often are sites requested to be blocked or unblocked? Periodically evaluate whether it is fit for purpose and involve all stakeholders in this process.
  In addition, bear in mind that 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 important that your ICT services are regularly reviewed, updated and removed if no longer in use. Installing the latest versions and patches often addresses security vulnerabilities without which your services might come under attack. Ensure that this is part of the job description of the ICT coordinator.

- You urgently need to get virus protection for devices that need to be protected on the school network and adopt consistent school-wide practice on virus protection. Just one infected device can contaminate the school's whole network and certain types of virus can even save illegal content to your server.
  You should also include 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. Check out the fact sheet on Protecting your devices against malware at www.esafetylabel.eu/group/community/protecting-your-devices-against-malware.

Pupil and staff access to technology

- 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.

- 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).

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.

- 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.

- You have a good policy of encrypting pupil data and storing it safely. Ensure all new staff made aware of the procedures for encryption and data handling and that there is a named point of contact acting as the data controller for your school. Upload to your school profile some guidelines about protecting sensitive data through an encryption system so that other schools can benefit from your experience.

Software licensing 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.

- There is a mechanism set up in your school that allows any staff member to make a request for new hard/software - a request that leads to an informed decision within a reasonable amount of time. This is great as this way teacher can benefit from new technologies while still staying inline with school policy.

Policy

Acceptable Use Policy (AUP)

- It is good that you have an Acceptable Use Policy (AUP) for pupils. You should now amend the AUP to include staff and the wider community. To ensure that your revised AUP is sufficiently comprehensive, take a look at the fact sheet and check list on Acceptable Use Policy at www.esafetylabel.eu/group/community/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?

- This is good teaching practice, but you need to consolidate it with a section dedicated to mobile phone usage in your School Policy and your Acceptable Use Policy. Consult all stakeholders to develop this; the fact sheets on Using mobile phones at school (www.esafetylabel.eu/group/community/using-mobile-device-in-schools) and School Policy (www.esafetylabel.eu/group/community/school-policy) will provide helpful information.

- 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

- 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.

- 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.

- 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

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

Pupil practice/behaviour

- 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

- While your school has an online presence, pupils cannot take part in shaping it. Explore if there could be a way to involve pupils, maybe as part of a digital council. 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.

- 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

- 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.

- All pupils need to receive some eSafety education. Although pupils may not be using technology within school, they will more than likely be using it at home and so some of the issues surrounding the use of online technology need to be addressed.

- While it is good that you discuss consequences of online actions terms and conditions, online payments and copyright with older pupils, consider discussing these also with young pupils.

- 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.

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/community/pupils-use-of-online-technology-outside-school.

Sources of support 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.

- 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.

- 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?

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.