eSafety Label - Action Plan

Action plan submitted by MELTEM UYAR for Milas Merkez Ortaokulu - 18.01.2023 @ 08:14:30

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

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

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.

Data protection

- 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.
- It is good that your school records are stored in a safe environment, it is also necessary that they are archived and disposed with in line with the Data Protection Act. Ensure that a good records management system is put in place. Check the according fact sheet for more information.
- Any data relating to pupils should be encrypted before it is sent or stored electronically. Investigate urgently how data can be protected, making use of other school's advisers or good practice guides, and take action. See the fact sheet on Protecting Sensitive Data (www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools).

Software licensing

- Compliance with licensing agreements is important. Someone needs to have overall responsibility to ensure that this is happening and that all licenses are valid for purpose. Staff should be briefed on who is the person responsible.
  The End-user license agreement section in Wikipedia will provide useful information for understanding terms and conditions and comparing software agreements.

- 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.

- Review the budget for software needs. You might also want to look into alternatives, e.g. Cloud services or open software.

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)

- There are no eSafety policies in your school. Policies and procedures are an essential part of the management of a school. They provide clear guidelines to staff and pupils on how to behave within school perimeters and also how to respond to incidents. Make the creation of the school policy and the Acceptable Use Policy (AUP) a priority. You can find more information on this in the eSafety factsheet area of the eSafety Label community.

- 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.

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).

- It is important to have a school-wide policy on handling issues when pupils knowingly or even inadvertently access illegal or offensive material online, since standards and practices can vary considerably from one teacher to the next. Guidance on this topic is provided on the teachtoday.de/en website (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.

Staff policy

- New technologies, such as smartphones or other mobile devices bring a new set of risks with them. Ensure that your teachers are aware of those. This way they can avoid the pitfalls when using the devices and also pass the knowledge onto the pupils.

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

- 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.

- Review the policy on taking photographs of, and by, pupils, parents and staff and check that it reflects any recent developments. Ideally, the policy should focus on behaviour rather than specific technologies. 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) will provide a good starting point.

- 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.

- 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.

Practice

Management of eSafety eSafety in the curriculum

- It is good that cyberbullying is a topic within the curriculum of older pupils. Unfortunately, however, it is also an issue that very young pupils are faced with. Try to discuss this with pupils from a very early age, maybe in the form of role plays. Also check the according fact sheet for more information.

- 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.

- 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.

- 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.

- Sexting is an issue which affects many young people. Sharing possible consequences and risks with them is important, as is the opportunity for some discussion around the issue. Sexting should be part of a broad and balanced eSafety curriculum.

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

Extra curricular activities

- Consider sharing the information you have about your pupils' online habits with other schools through the eSafety Label community. You could, for example, upload your latest survey findings on pupils' online habits to your school profile via your My school area.

Sources of support

- It is good that there is an informal network of 'eSafety expert' pupils in your school. Explore ways to strengthen this, maybe through optional courses and/or school rewards on eSafety topics or similar.

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.

- All staff need to be regularly updated about emerging trends in eSafety issues. Consider a needs-analysis to determine what different staff need from their training and consult the eSafety Label portal to see suggestions for training courses at www.esafetylabel.eu/group/community/suggestions-for-online-training-courses.

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.