

Action plan submitted by Gülcan Kaplan for sincik anadolu imam hatip lisesi - 06.02.2020 @ 15:36:07

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.

Pupil and staff access to technology

- › There are clear advantages for staff and pupils to bring their personal devices to school and to access internet on them. Besides supplementing the technical equipment available at school, this provides an important link between learning at home and at school and an opportunity to guide young people in responsible use. However, staff and pupil use of their own equipment on the school network needs to be addressed in an Acceptable Use Policy so that users are clear about which networks they should use and why. The Acceptable Use Policy needs to include clear guidance about which activities are permitted while on the school network, and what is not allowed.
- › 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.esafetylevel.eu/group/community/using-mobile-device-in-schools).

Data protection

- › It is good that your school provides training materials on the importance of protecting devices, especially

portable ones. Please consider sharing those with others through the in . Also ensure that your materials are regularly reviewed to ensure they are in line with the state of the latest technology.

- › 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.esafetylevel.eu/group/community/protecting-sensitive-data-in-schools).
- › Your new users are given a standard password and are asked to generate their own password on their first access. 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.esafetylevel.eu/group/community/safe-passwords.
Include these rules in your Acceptable User Agreement and avoid giving new users a standard "first access" password.

Software licensing

- › It is good that you can produce an overview of installed software and their licences in a short time frame with the help of several people. Consider centralising this.

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.
- › Once a year decisions on new hard/software are made. Investigate ways to also allow for new hard/software requests throughout the year. It will allow teachers to create a more engaging lesson without the temptation of unauthorized copying and its inherent dangers and costs.

Policy

Acceptable Use Policy (AUP)

- › 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.esafetylevel.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?
- › 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

- › Check that your School Policy includes all necessary information for teachers about handling issues when pupils knowingly or even inadvertently access illegal or offensive material online by going to the guidance set out by 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.
- › Please share the materials in which you tackle these issues especially with pupils and parents in the of the eSafety Label portal.

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.
- › 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 has a school wide approach of positive and negative consequences for pupil behaviour. This is good practice, please share your policy via the [My school area](#) of the eSafety portal so that other schools can learn from it.

School presence online

- › 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.
- › 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.esafetymodel.eu/group/community/acceptable-use-policy-aup-).

- › 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.

eSafety in the curriculum

- › 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.
- › 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.
- › It is good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.
- › In order to be ready for the world of today, pupils need to understand the legal consequences of their online actions. See if topics such as terms and conditions, online payments and copyright can be integrated into the 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 Embedding eSafety in the curriculum at www.esafetymodel.eu/group/community/embedding-online-safety-in-curriculum.

Extra curricular 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.

Sources of support

- › It is good to know that other school services are involved in eSafety issues (e.g. counsellors, psychologists, school nurse). Are they also invited to contribute to developing and regular review of your School Policy? Publish a case study about how this is managed in your school on your school profile page on the eSafety Label project website, so that others can learn from your experience.
- › It is great that you have a staff member which is knowledgeable in eSafety issues who acts as a teacher of confidence to pupils.

Staff training

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.