

Action plan submitted by hatice evren for nilüfer zübeyde hanım anaokulu - 09.01.2023 @ 06:45:00

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 very good that all your school devices 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/community/protecting-your-devices-against-malware](http://www.esafetylabel.eu/group/community/protecting-your-devices-against-malware).
- › It is good practice that your ICT services are regularly reviewed, updated and removed if no longer in use.

### 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.
- › 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](http://www.esafetylabel.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.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools](http://www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools)).

- › There is a retention plan in place for your school detailing how specific school records are stored, archived and disposed. This is very good. Ensure that the plan is followed and review it regularly to ensure it relates to the Data Protection Act and other relevant legislation. Check the according fact sheet for more information.

## 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.

## IT Management

- › 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.
- › It is good practise that your are training and/or providing guidance in the use of new software that is installed on school computers. This ensures that school members will take advantage of new features, but also that they are aware of security and data protection issues where relevant.

## Policy

### Acceptable Use Policy (AUP)

- › 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

- › 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](http://www.esafetylabel.eu/group/teacher/incident-handling)), as this enables schools to share and learn from each other's strategies.
- › 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.
- › 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

- › It is good practice that the school policy includes information about risks with potentially non-secured devices,

such as smartphones and that reference is made to it. Consider sharing your school policy via the uploading evidence tool, also accessible through the [My school area](#).

## Pupil practice/behaviour

- › Electronic communication guidelines for pupils should be clearly communicated in the Acceptable Use Policy. Communication between pupils can rapidly degenerate if standards are not set, giving rise to incidents such as cyberbullying. Learning about effective, responsible communication should also be part of the school curriculum, as it is a necessary competence for every young person. Discuss this at a staff meeting in order to define the standards you want to implement.
- › 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.
- › We recommend that you specifically nominate a web-experienced staff member to periodically check the school's online reputation. Monitoring such an important aspect on an ad hoc basis only is insufficient. Remember that this is the image that prospective parents will receive when they search for your school online.
- › 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](http://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

- › Ensure that the governor or board member appointed for eSafety has the opportunity to receive regular training and also to ensure that colleagues are aware of eSafety issues. Involve your governing body in the development and regular review of your School Policy. See our fact sheet on School Policy [www.esafetylabel.eu/group/community/school-policy](http://www.esafetylabel.eu/group/community/school-policy).
- › It is good that all staff in your school are responsible for eSafety. However, it is good practice to appoint a person who will have overall responsibility for eSafety issues to provide the focus needed. Ideally this should be someone from the senior leadership team. 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](http://www.esafetylabel.eu/group/teacher/incident-handling).

## eSafety in the curriculum

- › 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.
- › 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.
- › 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 that eSafety is taught as part of the curriculum in your school. Ensure that all staff are delivering eSafety education where appropriate throughout the curriculum and not just through ICT or Personal Social and Health lessons. You/your staff may find some useful ideas and resources in the fact sheet Embedding eSafety in the curriculum at [www.esafetylevel.eu/group/community/embedding-online-safety-in-curriculum](http://www.esafetylevel.eu/group/community/embedding-online-safety-in-curriculum).
- › It is good practice that all pupils in all year groups in your school are taught about eSafety. It continues to be important to review regularly the curriculum provision to ensure it meets ever-changing needs. If you have a curriculum review process of this kind, it would be helpful to other schools if you could publish this on your school profile. To upload go to your [My school area](#).

## 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.esafetylevel.eu/group/community/pupils-use-of-online-technology-outside-school](http://www.esafetylevel.eu/group/community/pupils-use-of-online-technology-outside-school).

## Sources of support

- › Young people are more open to advice from their peers. Consider offering optional courses and/or school rewards on eSafety topics or similar that stimulate expert knowledge in pupils that then could become a point of reference for their peers.

## Staff training

- › 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.