

Action plan submitted by ebru ulukuş for Polatlı Genç Osman Ortaokulu - 15.03.2021 @ 12:19:37

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.
- › 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.

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

- › It is good that your school provides materials on the importance of protecting devices, especially portable ones. Ensure that staff are aware of these and use them. This material should be pointed out to new staff as part of their induction. Please consider uploading those as evidence at [evidence](#) and sharing with others in the forum. Also ensure that your materials are regularly reviewed to ensure they are in line with the state of the latest technology.
- › 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.esafetylevel.eu/group/community/protecting-sensitive-data-in-schools.

- › 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).

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 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.

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.
- › 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)

- › 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 good that you have an Acceptable Use Policy for all members of the school community. Regularly review the AUP to ensure that it is still fit for purpose; to ensure that your AUP is sufficiently comprehensive, take a look at the fact sheet and check list on Acceptable Use Policy at www.esafetylevel.eu/group/community/acceptable-use-policy-aup-.

Reporting and Incident-Handling

- › Are all staff familiar with the procedure for dealing with material that could potentially be illegal? Is there a named person from the school senior leadership team who takes overall responsibility in this type of case? The procedure needs to be clearly communicated to all staff in the School Policy, and to staff and pupils in the Acceptable Use Policy. Remember to report and suspected illegal content to your 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.

- › Please share the materials in which you tackle these issues especially with pupils and parents in the of the eSafety Label portal.
- › It is good practice to log cyberbullying incidents that occur in your school centrally, as you are contributing to building a data base of successful incident handling practices from schools across Europe that you and others can use in future. Make sure that pupils sign up to anti-bullying guidelines in your Acceptable Use Policy.
- › It's good that you have a clear School Policy on handling out-of-school eSafety incidents; is the number of these declining? Start a discussion thread in the community on what other preventative measures or awareness raising activities could be used in order to reduce the number of issues further. 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.

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.
- › You have guidelines in your Acceptable Use Policy (AUP) on teachers' classroom usage of mobile phones. Upload your AUP to your school profile as it is a model of good practice that can help other eSafety Label schools.

Pupil practice/behaviour

- › You have defined electronic communication guidelines in your Acceptable Use Policy and this would be a useful example of good practice for other schools. Can you create a tutorial about electronic communication guidelines for pupils and upload it to your school profile via your [My school area](#) so that other schools can benefit from your experience.

School presence online

Practice

Management of eSafety

- › 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/community/school-policy.

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 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 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.esafetymodel.eu/group/community/embedding-online-safety-in-curriculum.

Extra curricular activities

- › It is good to know that you are frequently using the online eSafety resources from your national Safer Internet Centre. Have you found these resources helpful in your school? Please send your feedback on their use and value to info-insafe@eun.org.

Sources of support

- › Ask parents for feedback on the kind of eSafety support which is being provided for them and consider innovative ways to maximise the number of parents who are benefitting from, and accessing it. See the fact sheet Information for parents at www.esafetymodel.eu/group/community/information-for-parents to find resources that could be circulated to parents and ideas for parent evenings.
- › All staff should have some responsibility for eSafety. School counsellors, nurses, etc. are all well placed to provide advice and guidance on these issues and should be invited to contribute to developing and regularly reviewing your School Policy. Make the maximum use of their knowledge and skills and consider whether it is appropriate to provide training for them.
- › 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

- › 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](#).

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.

© 2021 European Schoolnet